

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005 年 8 月 25 日 (25.08.2005)

PCT

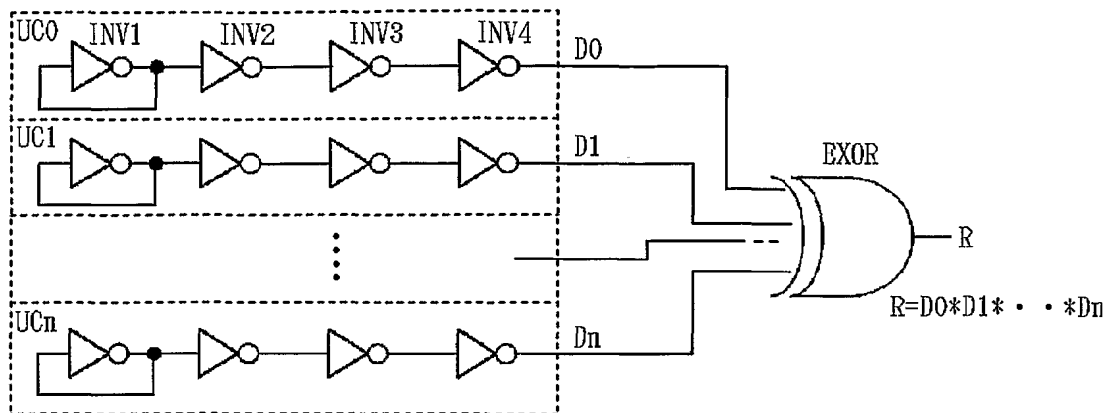
(10) 国際公開番号
WO 2005/078573 A1

- (51) 国際特許分類⁷: G06F 7/58 (74) 代理人: 徳若 光政 (TOKUWAKA, Kousei); 〒181-0001 東京都三鷹市井の頭5丁目16番8号 Tokyo (JP).
- (21) 国際出願番号: PCT/JP2004/001486 (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (22) 国際出願日: 2004 年 2 月 12 日 (12.02.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 株式会社日立超エル・エス・アイ・システムズ (HITACHI ULSI SYSTEMS CO., LTD.) [JP/JP]; 〒187-8522 東京都小平市上水本町5丁目22番1号 Tokyo (JP).
- (72) 発明者; および (75) 発明者/出願人 (米国についてのみ): 村中 雅也 (MURANAKA, Masaya) [JP/JP]; 〒187-8522 東京都小平市上水本町5丁目22番1号 株式会社日立超エル・エス・アイ・システムズ内 Tokyo (JP).
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) Title: RANDOM NUMBER GENERATING METHOD AND SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE

(54) 発明の名称: 乱数発生方法と半導体集積回路装置



(57) Abstract: A plurality of unit circuits each comprising first and second logic circuits formed into an identical shape through identical fabrication process, and an amplifier circuit for forming a binary signal by amplifying a noise being superposed on the differential voltage of threshold voltages of the first and second logic circuits, and a signal variation detecting circuit for forming an output signal in response to variation in any one of a plurality of binary signals being outputted from the plurality of unit circuits are provided and a random number is generated by combining a plurality of binary signals being outputted from the signal variation detecting circuit.

(57) 要約: 互いに同じ製造過程をもって同一の形態として形成された第1及び第2論理回路と、上記第1論理回路及び第2論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して2値信号を形成する増幅回路とからなる単位回路の複数個と、上記複数個の単位回路から出力される複数個からなる2値信号のうちのいずれか1つの信号変化にตอบสนองして出力信号を形成する信号変化検出回路とを備え、上記信号変化検出回路から出力される2値信号の複数個を組み合わせて乱数を生成する。



WO 2005/078573 A1



添付公開書類：
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

乱数発生方法と半導体集積回路装置

05 技術分野

この発明は、乱数発生方法と半導体集積回路装置に関し、主として半導体製造技術に好適な乱数発生方法及びその半導体集積回路装置に利用して有効な技術に関するものである。

10 背景技術

近年のネットワーク化及びIT化急速に拡大する社会において、暗号技術や認証技術等のセキュリティ技術の重要性が高まっている。それらの技術の重要な要素の一つとして乱数がしばしば用いられている。現在、数種類の基本原理に基づいた乱数発生回路が実用化されている。高度

15 情報セキュリティ向け超小型真性乱数生成回路の例として、「東芝レビュー」Vol.58・8(2003)（第1の先行技術）がある。また、特開2003-173254号公報（第2の先行技術）には、RSフリップフロップの電源をオンオフすることにより得られる不確定出力を利用する乱数生成回路が記載されている。

20

発明の開示

乱数発生回路の性能を比較する要素は、乱数の品位（不規則性）、回路面積、消費電力及び応答時間（新しい乱数を生成するために要する時間）などであるが、従来の乱数発生回路はいずれも一長一短を持っている。乱数には、コンピュータのアルゴリズムなどで乱数を発生させる擬

25 似乱数と、自然界の物理現象などを使って乱数を発生させる真性乱数の

二つがある。一般的に、後者の方の品位が高いとされている。真性乱数は、偶然性、非再現性、予測不可能性の特長を持っているが複雑な回路や素子を必要とし、簡便な装置への適用に適していない。例えば、上記第 1 の先行技術において提案されている技術は、真性乱数発生回路であるが、プロセス（エッチング工程）の変更及びその制御が必要となるものである。また、上記第 2 の先行技術は電源投入時の過渡的状況下での現象を利用するため、乱数の不規則性を低下させる要因が設計段階では予測不能であり、乱数の品質を保証することが困難であると考えられる。

したがって、この発明の一つの目的は、製造プロセスの変更を行うことなく、小面積で高い品位の乱数を生成することができる乱数発生方法及び乱数発生回路を備えた半導体集積回路装置を提供することにある。この発明の他の目的は、低消費電力化を実現した乱数発生方法及びかかる乱数発生回路を備えた半導体集積回路装置を提供することにある。この発明の前記ならびにそのほかの目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

本願において開示される発明のうち代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、互いに同じ製造過程をもって同一の形態として形成された第 1 及び第 2 論理回路と、上記第 1 論理回路及び第 2 論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して 2 値信号を形成する増幅回路とからなる単位回路の複数個と、上記複数個の単位回路から出力される複数個からなる 2 値信号のうちのいずれか 1 つの信号変化に応答して出力信号を形成する信号変化検出回路とを備え、上記信号変化検出回路から出力される 2 値信号の複数個を組み合わせ

て乱数を生成する。

図面の簡単な説明

第 1 図は、この発明に係る半導体集積回路装置に搭載される真性乱数発生回路の基本概念を示す回路図であり、

第 2 図は、第 1 図の真性乱数発生回路を説明する動作原理図であり、

05 第 3 図は、この発明に係る真性乱数発生回路の一実施例を示す基本的回路図であり、

第 4 図は、第 3 図の真性乱数発生回路の一実施例を示す具体的回路図であり、

10 第 5 図は、第 3 図の真性乱数発生回路の動作の一例を説明するための波形図であり、

第 6 図は、第 4 図の真性乱数発生回路の信号変化検出回路の一実施例を示す具体的回路図であり、

第 7 図は、この発明に係る真性乱数発生回路の他の一実施例を示す回路図であり、

15 第 8 図は、第 7 図の真性乱数発生回路の動作の一例を説明するための概念的な波形図であり、

第 9 図は、この発明に係る真性乱数発生回路とその要素回路の一実施例を示す回路図であり、

20 第 10 図は、この発明に係る真性乱数発生回路とその要素回路の他の一実施例を示す回路図であり、

第 11 図は、第 9 図の真性乱数発生回路の動作の一例を説明するための概略波形図であり、

第 12 図は、この発明に係る真性乱数発生回路の他の一実施例を示す概念図であり、

25 第 13 図は、第 12 図の初期値発生回路の一実施例を示す回路図であり、

第 1 4 図は、第 1 2 図の初期値発生回路の他の一実施例を示す回路図であり、

第 1 5 図は、第 1 3 図と第 1 4 図の初期値発生回路の動作を説明するための波形図であり、

05 第 1 6 図は、この発明に係る真性乱数発生回路の他の一実施例を示す回路図であり、

第 1 7 図は、この発明に係る真性乱数発生回路の一実施例を示す回路図であり、

第 1 8 図は、第 1 7 図の真性乱数発生回路に設けられたテスト回路の動作の一例を説明するためのタイミング図であり、

10 第 1 9 図は、この発明に係る真性乱数発生回路の一実施例を示す回路図であり、

第 2 0 図は、第 1 9 図の真性乱数発生回路の動作波形図であり、

第 2 1 図は、この発明に係る真性乱数発生回路の一実施例を示す回路図であり、

15 第 2 2 図は、この発明に係る真性乱数発生回路の出力部の他の一実施例を示す回路図であり、

第 2 3 図は、第 2 1 図に示した真性乱数発生回路の動作波形図であり、

20 第 2 4 図は、この発明に係る真性乱数発生回路の一実施例を示すチップ構成図であり、

第 2 5 図は、この発明に係る半導体集積回路装置の一実施例を示すブロック図であり、

第 2 6 図は、この発明に係る半導体集積回路装置の他の一実施例を示すブロック図であり、

25 第 2 7 図は、この発明に係る真性乱数発生回路の他の一実施例を示す

構成図であり、

第 28 図は、第 27 図に示した真性乱数発生回路の動作の一例を示す
タイミング図であり、

05 第 29 図は、この発明が適用される IC カードの一実施例を示す外観
図であり、

第 30 図は、この発明に係る IC カードに搭載される IC カード用チ
ップの一実施例を示す概略ブロック図であり、

第 31 図は、この発明が適用される非接触 IC カードの一実施例を示
すブロック図であり、

10 第 32 図は、この発明に係る真性乱数発生回路で生成された真性乱数
の 2 次元散布図であり、

第 33 図は、第 4 図の真性乱数発生回路の変形例を示す具体的回路図
であり、

15 第 34 図は、第 1 図に示した真性乱数発生回路の基本概念の変形例を
示す回路図であり、

第 35 図は、第 1 図に示した真性乱数発生回路の基本概念のさらに別
の変形例を示す回路図である。

発明を実施するための最良の形態

20 この発明をより詳細に説述するために、添付の図面に従ってこれを説
明する。

第 1 図には、この発明に係る半導体集積回路装置に搭載される真性乱
数発生回路の基本概念の回路図が示されている。第 1 図に示された CM
OS インバータ回路 INV1 ～ INV4 は、半導体集積回路装置の設計
25 及び製造の上では、現実的に制御可能な範囲内において、互いに同じ特
性を持つように構成される。複数のインバータを互いに同じ特性にする

ため技術について、以下に概略的に説明する。

CMOSインバータ回路において、その特性は、概略的には、それを構成するPチャンネル型MOSFETとNチャンネル型MOSFETとの相対的なコンダクタンスによって決まると理解されているであろう。

05 その観点ではチャンネル幅 W とチャンネル長 L との比 W/L は同じであるがサイズが異なるMOSFETによっても同じ特性のCMOSインバータを構成できると理解され得る。しかしながら、半導体集積回路装置の製造バラツキによる電気特性への影響は、異なったサイズの素子に対しては異なったものとなる。

10 この実施例では、かかる複数のCMOSインバータINV1～INV4のそれぞれは、好適には、それぞれを構成する素子の相互、すなわちPチャンネル型MOSFETの相互、及びNチャンネル型MOSFETの相互が互いに同じ構造、同じサイズを持って構成される。言うまでもなくそれら素子は、同じ素子は同じプロセスの下で一括製造されるという半導体集積回路装置の特徴に従って製造される。これによって複数のCMOSインバータINV1～INV4は、半導体集積回路装置の製造上の加工寸法のバラツキ、各種層の厚さバラツキ、不純物濃度バラツキ等々の製造バラツキによる影響を均等に受けるようにされる。

20 第1図のように入出力が短絡させられたCMOSインバータ回路INV1の出力電圧は、論理しきい値電圧に到達する。全てのCMOSインバータ回路が、完全に同じ電気的特性を持っていれば、4つのインバータ回路INV1～INV4の論理しきい値電圧は等しくなる。しかし、これは理想的な状態であり実際の半導体素子においては、僅かな特性の違いが存在するため、各インバータ回路INV1～INV4の論理しきい値電圧に差が生じる。

25 CMOSインバータ回路の論理しきい値のバラツキの要因としては、

MOSトランジスタ特性のバラツキが支配的であると捉えてよい。そして、MOSトランジスタ特性のバラツキの原因としては、MOSトランジスタのゲート幅や、ゲート絶縁膜膜厚、導電決定不純物濃度とその分布などを挙げることができる。これらのバラツキはマクロ的な部分とミ
05 クロ的とに分けることができる。マクロ的な部分としては、同一ロット内の複数のウェハ間のゲート幅バラツキなどである。

本願発明においては、主としてミクロ的な部分のバラツキを考慮するものであり、比較的に近接した位置に配置された素子間におけるバラツキについて検討した。このようなミクロ的なバラツキは、比較的に近接
10 した素子間にランダムに発生するものとして観測される。

すなわち、第1図のインバータ回路INV1、INV2の論理しきい値のバラツキもランダムであると考えられる。この論理しきい値のバラツキは、後述するように真性乱数を発生させる上で好ましいことではない反面、別の観点では半導体素子の持つ特徴的な特性のバラツキが固有
15 の識別情報として利用できる。つまり、CMOSインバータ回路を用いた場合には、論理しきい値に生じるバラツキがNチャンネル型MOSトランジスタの持つバラツキにPチャンネル型MOSトランジスタの持つバラツキが加えられたものと見做すことができ、バラツキ範囲が広くなり識別番号ないし識別情報の発生を効果的に行うようにすることができる。
20 る。しかし、このことは半導体素子の各ノードで発生する雑音に応答した真性乱数を発生させる上では好ましくないものとなる。

第1図に示した概念図では、4つのインバータ回路INV1～INV4を基本回路（又は単位回路）UC0として、CMOSインバータ回路INV1の入力と出力とを短絡して、インバータ回路INV1の論理し
25 きい値電圧VLT1を形成する。この論理しきい値電圧VLT1はインバータ回路INV2の入力に供給される。かかるインバータ回路INV

2においては、そのしきい値電圧 V_{LT2} を参照電圧として上記論理しきい値電圧 V_{LT1} との電圧比較と増幅動作を行う。そして、かかるインバータ回路 $INV2$ の出力信号は、縦列接続されたインバータ回路 $INV3$ と $INV4$ からなる増幅回路により更に増幅されて2値信号に変換される。

理想的な条件においては、基本回路の第1のインバータ回路 $INV1$ の短絡された入出力ノードの電圧（論理しきい値電圧 V_{LT1} ）と第2のインバータ回路 $INV2$ の論理しきい値電圧 V_{LT2} とは等しくなるように設計、製造されるが、実際には前記のようなプロセスバラツキが存在するため一致するとは限らない。

半導体内を電子が移動する際、不規則な動きをするため僅かであるが電気信号ノイズを発生させる。その現象は、第1のインバータ回路 $INV1$ にも第2のインバータ回路 $INV2$ にも発生するが、上記のように $V_{LT1} = V_{LT2}$ のような理想的な条件においては、第1のインバータ回路 $INV1$ の電気信号ノイズが第2のインバータ回路 $INV2$ により増幅され、第2のインバータ回路の出力信号は電気信号ノイズを反映して振幅する。電気信号ノイズは完全に無秩序な動きをするため、第2のインバータ回路 $INV2$ から得られる出力信号は真性乱数といえる。

つまり、第2図（a）に示すように、単位回路 $UC0$ の第1のインバータ回路 $INV1$ と第2のインバータ回路 $INV2$ の論理しきい値電圧 V_{LT1} 、 V_{LT2} とが一致している場合、電気信号ノイズ V_{nz} が反転増幅されて出力信号 V_{out} として取り出すことができる。なお、同図では第2のインバータ回路 $INV2$ の電気信号ノイズは省略し第1のインバータ回路 $INV1$ の電気信号ノイズ V_{nz} に含めている。このようにして、第1のインバータ回路 $INV1$ の電気信号ノイズ V_{nz} は第2のインバータ回路 $INV2$ により反転増幅される。さらに第2のインバータ回路

INV 2 の出力信号 V_{out} は、第 3 および第 4 のインバータ回路 INV 3, INV 4 によりさらに増幅され、第 4 のインバータ回路 INV 4 の出力では最終的に電源電圧レベルの振幅の論理レベルの情報が取り出せる。

05 しかし、電気信号ノイズ V_{nz} は極めて小さく、また実際には各インバータ回路 INV 1, INV 2 を構成する MOS トランジスタの特性は前記のような要因によってバラツキがあるため、基本回路 UC 0 の第 1 および第 2 のインバータ回路 INV 1, INV 2 の論理しきい値電圧 V_{LT1} , V_{LT2} は必ずしも等しいとはいえない。

10 つまり、第 2 図 (b) に示すように、単位回路 UC 0 の第 1 のインバータ回路 INV 1 と第 2 のインバータ回路 INV 2 の論理しきい値電圧 V_{LT1} , V_{LT2} との間に ΔV のようなプロセスバラツキによる差電圧 ΔV が存在し、上記電気信号電圧ノイズ V_{nz} の振幅より、上記第 2 のインバータ回路 INV 2 の論理しきい値電圧 V_{LT2} が常に大きい場合には、第 2 のインバータ回路 INV 2 の出力信号 V_{out} は常にハイレベル
15 となってしまう。したがって、上記単位回路 UC 0 を単独で見た場合には、第 2 のインバータ回路 INV 2 の出力信号 V_{out} が上記の電気信号ノイズ V_{nz} を反映すると常に保証されるものではない。

20 そこで、一般的には上記 2 つの論理しきい値電圧 V_{LT1} , V_{LT2} の上記のようなプロセスバラツキを補正する方向にトリミングや補償回路を付加することが考えられるが、回路が複雑になったり、消費電流が増大するなどの問題を有するものとなる。

25 本願発明者においては、トランジスタの特性のバラツキはランダムな正規分布であることに着目し、第 1 図の示したように、数多くの基本回路を観察すれば、第 1 インバータ回路 INV 1 と第 2 のインバータ回路 INV 2 の特性が極めて等しい組み合わせがある確率で存在し、そのよ

うな基本回路は第2図(a)に示したように電気ノイズ V_{nz} に敏感に反応するものとなることを見出した。

つまり、第2図(c)のしきい値電圧分布図に示したように、インバータ回路 $INV1$ 、 $INV2$ の論理しきい値電圧 V_{LT1} 、 V_{LT2} は、正規分布となることが知られている。2つのインバータ回路 $INV1$ と $INV2$ を組み合わせると、その差 $V_{LT1} - V_{LT2}$ はもとの論理しきい値電圧 V_{LT1} 、 V_{LT2} の分散の2倍の正規分布となる。電気信号ノイズ電圧 V_{nz} の振幅より、第1のインバータ回路と第2のインバータ回路の論理しきい値電圧の差 $V_{LT1} - V_{LT2}$ が小さい基本回路が存在する確率は、インバータ回路の論理しきい値電圧 V_{LT} の分散と、電気信号ノイズ電圧の振幅 V_{nz} で決まる。基本回路群中に含まれるノイズを電気信号のノイズを反映する基本回路の平均数は、基本回路群を構成する基本回路の数に、前記の確率を乗じた数である。

第1図において、 $UC0 \sim UCn$ のような複数の基本回路の出力 $D0 \sim Dn$ を排他論理和回路に代表されるような信号変化検出回路 $EXOR$ に入力すると、その出力 R は接続された基本回路 $UC0 \sim UCn$ の出力信号 $D0 \sim Dn$ の変化のいずれにも反応して反転する。

上記複数の基本回路 $UC0 \sim UCn$ の中に、第1インバータ回路と第2のインバータの特性が極めて等しい組み合わせの基本回路が少なくとも1つ以上存在するように決められた複数からなる基本回路群の各出力を、信号変化検出回路 $EXOR$ に入力する。すると、排他論理和回路のような信号変化検出回路 $EXOR$ の出力 R は、基本回路 $UC0 \sim UC1$ の出力 $D0 \sim Dn$ のうちのいずれか1つが変化すると反転する。すなわち、信号変化検出回路 $EXOR$ の入力が基本回路の出力である場合、出力はかかる基本回路の電気ノイズを反映した真性乱数となる。基本回路群に、第1インバータ回路と第2のインバータ回路の特性が極めて等し

い組み合わせの基本回路が複数存在しても、各基本回路どうしの電気信号ノイズに相関はないため、信号変化検出回路E X O Rの出力Rは同様に乱数であり、より品位の高い真性乱数を得ることができる。第1図に示した論理式 $R = D_0 * D_1 * \dots * D_n$ において、*の記号は排他的論理和記号を表す。

図3には、この発明に係る乱数発生回路の一実施例の基本的回路図が示されている。この実施例では、前記図1のインバータ回路I N V 1 ~ I N V 4が、2入力のナンド(N A N D)ゲート回路G 1 ~ G 4に置き換えられる。上記ゲート回路G 1は、一方の入力と出力とが結合される。このゲート回路G 1の共通化された入出力がゲート回路G 2の一方の入力と接続される。ゲート回路G 2の出力はゲート回路G 3の一方の入力に接続される。ゲート回路G 3の出力はゲート回路G 4の一方の入力に接続される。そして、これらのゲート回路G 1 ~ G 4の他方の入力には、動作制御信号A C Tが共通に供給される。

第1図のインバータ回路I N V 1 ~ I N V 4は、上記ナンドゲート回路G 1 ~ G 4のような論理ゲート回路の一種と見做すことができる。すなわち、入力信号を反転させる論理動作を行うものであるからである。第1図のようにインバータ回路I N V 1 ~ I N V 4を用いた場合には、インバータ回路I N V 1とI N V 2のように初段側においては論理しきい値電圧V L T付近で動作するものであり、電源電圧V D Dと回路の接地電位との間に直流電流を流すものとなる。本願発明では、前記のように素子のプロセスバラツキによる論理しきい値電圧の正規分布を利用するものであり、そのために比較的多数からなる単位回路を動作させる必要があるので、上記インバータ回路I N V 1とI N V 2での直流電流は低消費電力化を実現する上では無視できない。

これに対して、この実施例のようにゲート回路G 1 ~ G 4を用いた場

合には、各ゲート回路G 1～G 4は、動作制御信号A C Tをロウレベル（論理0）のような非活性化レベルとしたとき、上記動作制御信号A C Tとは異なる他方の入力信号に無関係に出力信号をハイレベル（論理1）にし、各ゲート回路G 1，G 2においても直流電流が発生しない。すなわち、この実施例回路では、乱数を必要とするタイミングで上記動作制御信号A C Tをハイレベル（論理1）のような活性化レベルとする。これにより、各ゲート回路G 1～G 4は、上記動作制御信号A C Tとは異なる他方の入力信号に応答して反転信号を形成するというインバータ回路としての動作を行う。これにより、上記動作制御信号A C Tをハイレベルにすることにより、第1図の基本回路図と同様の動作を行うものとなる。

第4図には、第3図の真性乱数発生回路の一実施例の具体的回路図が示されている。ゲート回路G 1は、出力ノードN 1と回路の接地電位V S Sとの間に直列形態にされたNチャネルM O S F E T Q 1とQ 3、上記出力ノードN 1と電源電圧V D Dとの間に並列形態にされたPチャネルM O S F E T Q 2とQ 4から構成される。上記M O S F E T Q 1とQ 3のゲートが共通に接続されて第1の入力とされる。上記M O S F E T Q 2とQ 4のゲートが共通に接続されて第2の入力とされる。他のゲート回路G 2～G 4も上記と同様な回路により構成される。

上記ゲート回路G 1～G 4は、半導体集積回路装置の設計及び製造の上では、現実的に制御可能な範囲内において、互いに同じ特性を持つように構成される。複数のゲート回路を互いに同じ特性とする技術について、以下に概略的に説明する。ゲート回路G 1～G 4において、その特性である論理しきい値は、概略的には、それを構成するPチャネルM O S F E TとNチャネルM O S F E Tとに決まると理解されているであろう。その観点ではチャネル幅Wとチャネル長Lとの比 W/L は同じであ

るがサイズが異なるMOSFETによっても同じ特性のCMOSゲート回路を構成できると理解され得る。しかしながら、半導体集積回路装置の製造バラツキによる電気特性への影響は、異なったサイズの素子に対しては異なったものとなる。

05 この実施例では、かかる複数のゲート回路G1～G4のそれぞれは、好適には、それぞれを構成する素子の相互、すなわちPチャネル型MOSFETの相互、及びNチャネル型MOSFETの相互が互いに同じ構造、同じサイズを持って構成される。言うまでもなくそれら素子は、同じ素子は同じプロセスの元で一括製造されるという半導体集積回路装置
10 の特徴に従って製造される。これによって複数のゲート回路G1～G4は、半導体集積回路装置の製造上の加工寸法のバラツキ、各種層の厚さバラツキ、不純物濃度バラツキ等々の製造バラツキによる影響を均等に受けるようにされ、かつ、論理しきい値電圧も正規分布を持つようにされる。

15 第3図に示した実施例では、2つのゲート回路G1とG2の論理しきい値の大きさの判定出力がゲート回路G2から出力される。かかる信号伝達及び増幅経路に前記のような電気信号ノイズが重畳することにより、かかる電気信号ノイズに反映した出力信号を得る。つまり、ゲート回路G1の短絡された入出力ノードの電圧（論理しきい値に相当する）を
20 ゲート回路G2の入力バイアスとして供給し、上記電気信号ノイズに反映した出力信号を後段のゲート回路G3、G4により増幅してCMOSレベルの2値信号を得るものである。したがって、厳密にはゲート回路G3とG4は、単に増幅動作を行うものであるからゲート回路G1とG2のようにPチャネル型MOSFETの相互、及びNチャネル型MOSFETの相互が互いに同じ構造、同じサイズを持って構成される必要は
25 無いが、この実施例では主に回路設計の観点から同じ構造、同じサイズ

を持って構成される。

第5図には、上記第3図の真性乱数発生回路の動作の一例を説明するための波形図が示されている。同図では、信号伝達経路での電気信号ノイズは省略されている。動作制御信号ACTをロウレベルからハイレベルに変化させると、上記各ゲート回路G1～G4が実質的に動作状態となり、ゲート回路G1の出力ノードN1がその論理しきい値に対応した電圧にされる。なお、これに必要な時間を収束時間と呼ぶことにする。ゲート回路G2は、その論理しきい値によってノードN1の電圧を判定し、その出力ノードN2の電位を決める。この例では、ゲート回路G1の論理しきい値が、ゲート回路G2の論理しきい値によりも僅かに大きいので、ゲート回路G2での増幅動作によってノードN2の電位が上記ノードN1に対して小さい電圧にされる。このノードN2の電圧は、ゲート回路G3により増幅されてノードN3のようにハイレベルに大きくされる。そして、ゲート回路G4により更に増幅されてノードN4のように回路の接地電位VSSに到達する。

上記ノードN1とN2の電位差が僅かであり、そこに発生する電気信号ノイズがノードN2の電位以下になると、出力信号は反転するものとなる。つまり、前記第2図(a)と同様にノードN1とN2の電位差を反転させるような電気信号ノイズが発生した場合、逆にいうなら電気信号ノイズによりノードN1とN2の電位差関係が逆転してしまうような僅かの電圧差しかないゲート回路G1とG2の組み合わせを持つ基本回路では、出力はかかる基本回路の電気ノイズを反映した真性乱数を発生させることができる。当然のことであるが、上記の真性乱数を発生させることができるのは、収束時間を経過して後であることは言うまでもない。収束時間中であれば、各ナンドゲートのノードの過渡的な状態の影響を受け、本来の微小な電気ノイズを反映した真性乱数を得ることは難

しい。

この実施例では、回路が停止状態すなわち動作制御信号ACTがロウレベルであるとき、第3図のNチャンネルMOSFETQ3、Q7、Q11、Q15がオフ状態となり、前記のCMOSインバータ回路を用いた場合のような貫通電流が抑制される。また、ゲート回路としてナンド（NAND）回路を用いた利点は、CMOS論理LSIの標準素子であるため、適用する製品を限定しないことである。つまり、完全論理記述型回路で構成されるため、回路設計が容易になるものである。

第4図の実施例では、動作制御信号ACTが直列のNチャンネルMOSFETのQ3、Q7、Q11、Q15のゲートに接続されているが、NチャンネルMOSFETQ1、Q5、Q9、Q13に接続されて、ノードN1、N2、N3はNチャンネルMOSFETのQ3、Q7、Q11、Q15のゲートに接続されてもよい。

トランジスタレベル回路記述において重要なのは、個々のNAND素子中のMOSFETの信号接続位置である。上記の停止状態では各ゲート回路G1～G4の出力すなわちノードN1、N2、N3の電位が自動的に電源電圧となるため、それら信号の接続先のPチャンネルMOSFETのNBTIによる特性の変動を防止できる効果がある。

MOSトランジスタは、そのしきい値電圧が電界強度と温度とに依存するような電界ストレスによって不所望に変動することが有る。特にNBTI (Negative Bias Temperature Instability) と称される現象は、Pチャンネル型MOSFETで顕著に現われる現象である。この防御策として、目的外の時間においてPMOSのゲートに印加される電圧を高い電圧にする方法がよく用いられる。この実施例では、上記動作制御信号ACTのハイレベルにより論理しきい値判定動作を行わせ、かかる論理しきい値判定動作以外の時には、動作制御信号ACTをロウレベルにし

てPチャネル型MOSFETのゲートには、電源電圧を供給するようにゲート電圧を固定電圧にするものである。これにより、Pチャネル型MOSFETは、ゲート、ドレイン及びソースと基板（チャネル）の全てが電源電圧に等しい同電位となり、上記MOSFETの経時変化による論理しきい値の変動が極力抑えられる。このことは、前記のように各単位回路の出力信号を組み合わせによって識別情報を得る上で特に有効なものとなる。

これに対して、乱数発生回路においては、上記のような素子特性の変動、あるいは電源電圧の変動等には基本的には影響されないという特徴を有している。この実施例の乱数発生回路では、前記説明したように比較的多数の単位回路の中で少なくとも1個、ゲート回路G1とG2の論理しきい値電圧が前記電気信号ノイズからみて等しいものと見做されるものが存在すればよい。上記素子特性の変動、あるいは電源電圧の変動等には上記多数からなる単位回路群の全てにおいて発生し、それによりある単位回路ではゲート回路G1とG2の論理しきい値電圧が前記電気信号ノイズからみて等しいものと見做されていたものが外れても、別の単位回路では逆にゲート回路G1とG2の論理しきい値電圧が前記電気信号ノイズからみて等しいものと見做されることになるからである。

第33図には、第4図の真性乱数発生回路の変形例が示されている。第33図(a)のナンドゲート回路G1とG2（前記第1図のインバータ回路INV1とINV2に相当）の電気的特性バラツキを抑えるため、NANDを構成するトランジスタのチャネル長Lおよびチャネル幅Wをいずれも標準サイズ（通常プロセスの最小寸法）よりも大きくする。かかるトランジスタのLおよびWを大きくすることで、トランジスタのゲート電極の加工誤差に起因する特性のバラツキを抑えることができる。また、MOSトランジスタのゲート電極直下の不純物濃度の統計的変

動に起因するバラツキ（これを、「ゆらぎ現象」という。）を抑えることができる。近年の先端プロセスでは、同一チップ上のMOSトランジスタの電気的特性バラツキは、加工誤差よりのゆらぎ現象の影響が支配的であることが知られている。

- 05 ナンドゲート回路G 1 とG 2 を構成する各トランジスタ大きさは共通である必要はないが、回路動作時の状態に関わる、言い換えるならば上記活性状態での論理しきい値の決定に影響を及ぼすPチャネルMOSFET Q 2（Q 6）とNチャネルMOSFET Q 1，Q 3（Q 5，Q 7）を優先して大きくする。各ナンドゲート回路G 1 とG 2 の対応するMOSFETは同じ形状である必要がある。
- 10

また、増幅回路として動作するゲート回路G 3 及びG 4 は、上記のように設定することは必要ないが、回路設計上あるいは素子レイアウト上はゲート回路G 1 とG 2 と同様のものを用いるのが簡単となるし、後述するような乱数発生回路の存在を隠す上で有利なものとなる。

- 15 第33図（b）には、第33図（a）と同様の効果が得られる別の実現方法の回路が示されている。すなわち、3入力NANDゲートを用いて、活性状態での論理しきい値の決定に影響を及ぼすPチャネルMOSFETとNチャネルMOSFETを各2個ずつとし、上記ゆらぎ現象の影響を抑えるものである。これは、特殊なサイズのMOSトランジスタ
- 20 を特別に設計することなしに標準的なサイズのゲート部品で実現できるという利点がある。

- なお、前記第3図、第4図及び第33図はいずれもナンド（NAND）ゲートを用いて基本回路を構成したが、ナンドの代わりにノア（NOR）ゲートであっても構わない。ただし、その場合にはかかる基本回路
- 25 は、動作制御信号ACTがロウレベル（論理0）で活性化するものとなる。前記のように、NBTIと称される電界ストレスに起因する劣化現

象は特にPチャネルMOSFETで顕著である。しかし他の素子、例えばポリシリコンFETや有機トランジスタ等において、かかる劣化現象がPチャネル型ではなくNチャネル型で顕著である場合は、ノア（NOE）ゲートを用いることが望ましい。

- 05 なお、第3図に示される実施例において、各単位回路UC0～UCn内のナンドゲートG2，G3，G4については、それぞれに接続された共通制御信号ACTを電源VDDに接続して常にハイレベル（論理1）としてもよく、それによって本実施例の持つ基本的機能は変わらない。

- 10 第6図には、第3図の真性乱数発生回路の信号変化検出回路EXORの一実施例の具体的回路図が示されている。この実施例では、排他的論理和回路EX0～EXnが縦列接続されて上記信号変化検出回路EXORが構成される。単位回路UC0の出力信号D0を受ける排他的論理和回路EX0の他方の入力には、特に制限されないが、ロウレベル（論理0）のような固定値が与えられる。次段の単位回路UC1の出力信号D0
- 15 0を受ける排他的論理和回路EX1の他方の入力には、上記排他的論理和回路EX0の出力信号が供給される。以下、n+1番目の単位回路UCnの出力信号Dnを受ける排他的論理和回路EXnの他方の入力には、図示しないが1つ前の排他的論理和回路EXn-1の出力信号が供給される。

- 20 これにより、排他的論理和回路EXnの出力信号Rは、上記n+1個の単位回路UC0～UCnの出力信号D0～Dnの中のいずれか1つでも変化すると、それに対応してそれに対応した排他的論理和回路EXの出力信号が変化し、上記直列形態にされた排他的論理和回路によって出力信号Rが変化するものとなる。つまり、上記出力信号Rは、単位回路
- 25 （基本回路）の電気ノイズを反映した真性乱数となる。

上記信号変化検出回路EXORとしては、論理ゲート回路で構成する

場合には上記のような複数個の排他的論理和回路を用いるものが便利であるが、それに限定されず、出力信号 $D_0 \sim D_n$ の論理レベルの変化を検出するものであれば何であってもよい。例えば、出力信号 $D_0 \sim D_n$ と、その遅延信号により1ショットパルスを形成するもの等種々の実施形態を採ることができる。

第7図には、この発明に係る真性乱数発生回路の他の一実施例の回路図が示されている。この実施例では、単位回路 $UC_0 \sim UC_n$ がデコーダDECを用いて時間的に分散して動作させられる。そして、1つの排他論理和回路EXと、1つのフリップフロップ回路FFとを用いて、複数の単位回路 $UC_0 \sim UC_n$ の出力の排他論理を累算することにより真性乱数RRを得るものである。なお、排他論理和を複雑な論理に変更することで、発生パターンをより解読され難い真性乱数を得ることができる。

上記デコーダDECは、特に制限されないが、カウンタとデコーダにより構成される。つまり、クロックCLKをカウンタで計数して、その計数出力をデコードして単位回路 $UC_0 \sim UC_n$ を順次動作状態にする動作制御信号 $DEC_0 \sim DEC_n$ を生成するものである。あるいは、シフトレジスタを用い、選択信号に対応した初期値をクロックCLKにより順次にシフトして単位回路 $UC_0 \sim UC_n$ を順次に動作状態にする動作制御信号 $DEC_0 \sim DEC_n$ を形成するようにされる。

このように単位回路 $UC_0 \sim UC_n$ を順次に動作状態にするために、単位回路 UC_0 を例にして説明すると、ゲート回路G1とG2に対して動作制御信号としてのデコード出力 DEC_0 が供給される。増幅回路としてのゲート回路G3とG4は、上記ゲート回路G1とG2が動作制御信号 DEC_0 により動作状態とされたときには、それに対応した出力信号の増幅動作を行い、上記ゲート回路G1とG2が動作制御信号DEC

0により非動作状態とされたときには、前段の単位回路の出力信号をスルして伝達する動作を行う。

ゲート回路G 3の一方の入力には、それに対応したゲート回路G 2の出力信号が伝えられ、他方の入力には前段の単位回路の出力信号が伝えられる。ゲート回路G 4は、一方の入力にはそれに対応したゲート回路G 3の出力信号が供給され、他方の入力には電源電圧に対応されたハイレベルが固定的に供給される。これにより、ゲート回路G 4は実質的にはインバータ回路として動作する。初段の単位回路UC 0のゲート回路G 3の他方の入力には、電源電圧に対応されたハイレベルが固定的に供給される。

第8図には、第7図の真性乱数発生回路の動作の一例を説明するための概念的な波形図が示されている。デコーダDECにより、初段の単位回路UC 0に対応した動作制御信号DEC 0がハイレベルの選択レベルにされると、ゲート回路G 1とG 2による出力信号が形成されてゲート回路G 3, G 4により増幅されて出力信号D 0が形成される。単位回路UC 1～UC nにおいては、上記動作制御信号DEC 1～DEC nがロウレベルの非選択レベルであるので、ゲート回路G 2に相当するゲート回路の出力信号は全てハイレベルにされる。それ故、ゲート回路G 3に相当するゲート回路はインバータ回路としての動作を行い、前段回路からの出力信号を増幅するのみとなる。この結果、上記初段の単位回路UC 0の出力信号D 0は、上記単位回路UC 1～UC nのゲート回路を通して排他的論理和回路EXに伝えられる。つまり、D 1～D nは、D 0に従ったレベルにされる。

デコーダDECにより、第2番目の単位回路UC 1に対応した動作制御信号DEC 1がハイレベルの選択レベルにされると、上記同様にゲート回路G 1とG 2に対応した2つのゲート回路による出力信号が形成さ

れてゲート回路G 3, G 4に対応したゲート回路により増幅されて出力信号D 1が形成される。つまり、上記初段の単位回路では、選択信号DEC 0のロウレベルによりゲート回路G 2の出力信号がハイレベルとなり、出力信号D 0をハイレベルに固定する。したがって、上記のように
05 の単位回路UC 1においては、上記のようにゲート回路G 3, G 4に対応したゲート回路による増幅動作が行われる。以下、その出力信号D 1は、前記同様に後段側の単位回路における増幅回路としてのゲート回路を通して排他的論理和回路EXに伝えられる。つまり、D 2～D nは、D 1に従ったレベルにされる。第3番目以降の単位回路UC 2～UC n
10 の選択動作も前記同様である。

第7図の実施例回路の実際の波形は、第8図とは異なる。つまり、単位回路UC 0において非選択状態のときには、出力信号D 0がハイレベルにされる。つまり、上記DEC 1が非選択レベルになると同時に出力信号D 0は非選択状態に対応したハイレベルの出力信号を形成するもの
15 となる。このことは、単位回路UC 1～UC nが非選択レベルにされたときに、各出力信号D 1～D nも一斉にハイレベルにされる。このような非選択状態に対応して出力信号D 0～D nのレベルを忠実に表現すると、上記単位回路UC 0～UC nが順序動作し、その出力が順次（シリアル）に出力されることが解り難くなるので、単位回路UC 0～UC n
20 における非選択状態での出力レベルの変化を無視して第8図のように表すものである。

第7図の実施例回路において、 $(n+1)$ 個の単位回路（基本回路）を含む単位回路群が例示されており、 $(n+1)$ 個の基本回路の中に、第1ゲート回路G 1（第1インバータ回路INV 1）と第2ゲート回路
25 G 2（第2のインバータ回路INV 2）の特性が極めて等しい組み合わせの単位回路が少なくとも1つ以上存在する。前述のように、単位回路

群中に含まれる第1ゲート回路G1と第2ゲート回路G2の特性が極めて等しい組み合わせの単位回路の数が多いほど、得られる乱数の品位は高くなる。単位回路群に含まれる第1ゲート回路G1と第2ゲート回路G2の特性が極めて等しい組み合わせの単位回路の数を十分な数にするためには、第1ゲート回路G1と第2ゲート回路G2の特性が極めて等しい組み合わせの単位回路が存在する確率を上げ、単位回路群に含まれる単位回路数を、かかる確率に見合う適正な数にすることが必要である。第1ゲート回路G1と第2ゲート回路G2の特性が極めて等しい組み合わせの単位回路が存在する確率は、当該回路の製造プロセスと設計手法等に依存する要素が高い（出来高次第）ため、単位回路群に含まれる単位回路数の最適化が重要である。

また、乱数の品位を向上させる別の手段として、排他論理和回路EXとフリップフロップ回路FFを用いた累算の回数を増やすことも有効である。具体的には、第8図例示された動作波形において、 $(n+1)$ 個の単位回路の累算を、例えば $(n+1) \times m$ と m 倍に延長する。つまり、単位回路UC0～UCnの前出力D0～Dnを m 回にわたって読み出して1ビットの乱数R(RR)を決定するものである。

第9図には、この発明に係る真性乱数発生回路とその要素回路の一実施例の回路図が示されている。第9図(a)に示される真性乱数発生回路では、第9図(b)に示されるような単位回路（要素回路）が $M \times N$ 個のようにマトリックス配置される。

1つの行が前記第7図の回路のように接続され、その出力部に行選択信号により選択されるナンドゲート回路G0とクロックドインバータ回路CN0が設けられる。M個からなる各行を構成する単位回路は、対応するもの同士が列デコーダにより形成された列選択信号C0～CM-1により共通に選択される。上記N個の行方向に配置された単位回路は、

行デコーダにより形成された行選択信号 $R_0 \sim R_{N-1}$ により 1 つが選択される。かかる行選択信号 $R_0 \sim R_{N-1}$ は、上記ナンドゲート回路 G_0 とクロックドインバータ回路 C_{N0} からなる行選択回路の選択信号としても用いられる。選択回路を構成するクロックドインバータ回路 C_{N0} は、それが非動作状態のときに出力ハイインピーダンス状態になる
05 ので、上記 N 個のクロックドインバータ回路の出力信号が共通に接続され、選択された 1 つの行に対応したクロックドインバータ回路の出力信号がナンドゲート回路 G_{11} に伝達される。

動作制御信号 ACT によりゲートが制御されるナンドゲート回路 G_{10} とインバータ回路 INV_{10} を通してクロック CLK が M 進カウンタ
10 に供給される。これにより、 M 進カウンタでは動作制御信号 ACT が活性状態のときにクロック CLK に対応して $0 \sim M-1$ の計数動作を行い、列デコーダにより $C_0 \sim C_{M-1}$ の選択信号が形成されて単位回路の出力信号が第 7 図の実施例と同様にシリアルに出力される。

15 上記 M 進カウンタのキャリー信号が N 進カウンタに供給されるので、 N 進カウンタは M 進カウンタの 1 回りに対応して計数動作を行う。これにより、上記行方向に配置された M 個の単位回路の読み出しが行われると、行選択の切替が行われて 0 行目から R_{N-1} 行目まで、それぞれ N 個の単位回路の読み出しが実施される。

20 本実施例において、 $M \times N$ サイクルで全ての単位回路の読み出しが行われるから、 $M \times N$ サイクルにより出力 RR から 1 ビットの真性乱数を生成することができる。これを K 回繰り返すことにより K ビットの真性乱数を得ることができる。この構成では、 $M \times N$ 個の単位回路の中に少なくとも 1 つだけ前記のような電気信号ノイズに応答する単位回路が存在
25 するように $M \times N$ の数を選ぶものである。なお、上記 K 回の繰り返しの間に J 個 ($0 < J < K$ の整数) の乱数を取り出してもよい。ただしそ

の場合は、各乱数ビットの取り出しサイクルは $M \times N$ サイクル以上離れていなければならない。また、上記 M 個からなる単位回路の中に、前記真性乱数を発生させるものが少なくとも1つ存在するように M の数を選ぶものとする、 M サイクル毎（各行毎）に1ビットの真性乱数 R_R を取得することができるので、 $M \times N$ サイクルにより N ビットの真性乱数を発生させる真性乱数発生回路を構成することができる。

第9図（b）には、前記第9図（a）における回路要素の一実施例の具体的回路図が示されている。単位回路は、前記第7図に示したゲート回路 $G_1 \sim G_4$ に、行／列選択機能を設けるためのゲート回路 G_5 と G_6 が追加される。ナンドゲート回路 G_5 の2つの入力には、列選択信号 C_i と、行選択信号 R_i が供給される。ゲート回路 G_3 には、前記第7図の単位回路と同様にその行における1段前の単位回路の出力信号 D_i が供給される。これにより、行及び列が選択状態にされた1つの単位回路のみが前記のような動作状態にされる。

第9図（c）には、前記第9図（b）における回路要素の他の一実施例の具体的回路図が示されている。単位回路は、第9図（b）および前記第7図に示したゲート回路 $G_1 \sim G_4$ を3入力ナンドゲートにして、行／列選択機能を合わせ持たせている。ナンドゲート回路 G_5 および G_6 の3つの入力のうち2つの入力には、列選択信号 C_i と、行選択信号 R_i が供給される。ゲート回路 G_7 には、第9図（b）および前記第7図の単位回路と同様にその行における1段前の単位回路の出力信号 D_i が供給される。これにより、行及び列が選択状態にされた1つの単位回路のみが前記のような動作状態にされる。

第9図（a）におけるクロックインバータ回路 C_N は、第9図（d）に示すように、電源電圧 V_{DD} と回路の接地電位 V_{SS} との間に直列接続されたPチャネルMOSFET Q_1 、 Q_2 とNチャネルMOSFET

TQ 4、Q 3 から構成される。P チャンネル MOS FET Q 1 と N チャンネル MOS FET Q 3 のゲートが共通に接続されて入力端子 A とされる。P チャンネル MOS FET Q 2 と N チャンネル MOS FET Q 4 のドレインが共通に接続されて出力端子 B とされる。そして、端子 C から供給される制御信号は、N チャンネル MOS FET Q 4 のゲートに供給され、上記
05 制御信号がインバータ回路 I N V 1 2 によって反転されて P チャンネル MOS FET Q 2 のゲートに供給される。

端子 C から供給される行選択信号のような選択信号がハイレベルのときに N チャンネル MOS FET Q 4 と P チャンネル MOS FET Q 2 がオン
10 状態となり、入力端子 A からの入力信号を受ける N チャンネル MOS FET Q 3 と P チャンネル MOS FET Q 1 のオン／オフに対応した出力信号が出力端子 B から出力される。端子 C から供給される行選択信号のような選択信号がハイレベルのときに N チャンネル MOS FET Q 4 と P チャンネル MOS FET Q 2 が同時にオン状態となり、入力端子 A からの入力
15 信号により N チャンネル MOS FET Q 3 又は P チャンネル MOS FET Q 1 が相補的にオン状態となり、ロウレベル又はハイレベルが出力端子 B から出力される。

また、第 9 図 (a) におけるクロックドインバータ回路 C N は、第 9 図 (e) に示されるようなトランスファゲート回路であってもよい。クロックドインバータ回路 C N は、第 9 図 (e) に示すように、入力端子 A と出力端子 B との間に直列接続された P チャンネル MOS FET Q 5 と、N チャンネル MOS FET Q 6 から構成される。端子 C から供給される制御信号は、N チャンネル MOS FET Q 6 のゲートに供給され、上記制御信号がインバータ回路 I N V 1 4 によって反転されて P チャンネル MOS FET Q 5 のゲートに供給される。端子 C から供給される行選択信号
20 のような選択信号がハイレベルのときに P チャンネル MOS FET Q 5 と
25

NチャンネルMOSFETQ6がオン状態となり、入力端子Aからの入力信号が出力端子Bから出力される。端子Cから供給される行選択信号のような選択信号がハイレベルのときにNチャンネルMOSFETQ4とPチャンネルMOSFETQ2が同時にオン状態となり、入力端子Aからの
05 入力信号によりNチャンネルMOSFETQ3又はPチャンネルMOSFETQ1が相補的にオン状態となり、ロウレベル又はハイレベルが出力端子Bから出力される。また、端子Cから供給される行選択信号のような選択信号がロウレベルのときにNチャンネルMOSFETQ4とPチャンネルMOSFETQ2が同時にオフ状態となり、出力端子Bはハイインピー
10 ダンスとなる。

第10図には、この発明に係る真性乱数発生回路とその要素回路の他の一実施例の回路図が示されている。第10図(a)に示される真性乱数発生回路では、第10図(b)に示される単位回路がM(列)×N(行)個のようにマトリックス配置される。1つの行が前記第7図の回路
15 のように接続され、その出力部にナンドゲート回路G0と排他的論理和回路EX0が設けられる。ナンドゲート回路G0の他方の入力電源VDDが接続され常にハイレベル(論理1)状態である。M個からなる各行を構成する単位回路は、対応するもの同士が列デコーダにより形成された列選択信号C0～CM-1により共通に選択される。

20 動作制御信号ACTによりゲートが制御されるナンドゲート回路G10とインバータ回路INV10を通してクロックCLKがM進カウンタに供給される。これにより、M進カウンタでは動作制御信号ACTが活性状態のときにクロックCLKに対応して0～M-1の計数動作を行い、列デコーダによりC0～CM-1の選択信号が形成されて、N行で構
25 成されるCiを共通とする各行の単位回路の出力信号が第7図の実施例と同様にシリアルに出力される。

ナンドゲート回路G 0 の出力は、排他的論理和回路E X 0 に接続され、E X 0 の他方の入力には接続される。さらに排他的論理和回路E X 0 の出力は、となりの行の排他的論理和回路へ接続され、全ての行の排他的論理和回路の出力は順次となりの行へ縦列接続される。排他的論理和回路E X 0 の他方の入力には、特に制限されないが、ハイレベル（論理1）のような固定値が与えられる。これにより、縦列接続された排他的論理和回路の出力信号R A は、上記選択されたC i を共通とするN行の単位回路から生成されるN個の出力信号の中のいずれか1つでも変化すると、それに対応して各行の排他的論理和回路の各出力信号が変化し、上記縦列形態にされた排他的論理和回路によって出力信号R A が変化するものとなる。つまり、上記出力信号R A は、1サイクルの動作でN個の単位回路（基本回路）の電気ノイズを反映した値となる。

本実施例において、Mサイクルで全ての単位回路の読み出しが行われるから、Mサイクルにより出力R R から1ビットの真性乱数を生成することができる。これをK回繰り返すことによりKビットの真性乱数を得ることができる。この構成では、M×N個の単位回路の中に少なくとも1つだけ前記のような電気信号ノイズに応答する単位回路が存在するようにM×Nの数を選ぶものである。なお、上記K回の繰り返しの間にJ個（ $0 < J < K$ の整数）の乱数を取り出してもよい。ただしその場合は、各乱数ビットの取り出しサイクルはMサイクル以上離れていなければならない。

第10図（b）には、前記第10図（a）の真性乱数発生回路における回路要素の一実施例の具体的回路図が示されている。ナンドゲート回路G 1 とG 2 の2つの入力的一方には、列選択信号C i が供給される。ゲート回路G 3 には、前記第7図の単位回路と同様にその行における1段前の単位回路の出力信号D i が供給される。これにより、列が選択状

態にされた 1 つの単位回路のみが前記のような動作状態にされる。

第 11 図には、第 9 図の真性乱数発生回路の動作の一例を説明するための概略波形図が示されている。動作制御信号 A C T がハイレベルの活性化レベルにされた状態で、クロック C L K を入力すると、それに対応して列選択信号 C 0 ~ C M - 1 が列デコーダから出力される。このとき、N 進カウンタは計数值がゼロであるから 0 行目の行選択信号 R 0 を選択レベルにするので、第 0 行目の単位回路の出力信号が列選択信号 C 0 ~ C M - 1 に対応してシリアルに出力される。0 行目の単位回路の読み出しが行われると、そのキャリー信号により N 進カウンタが + 1 の計数動作を行い、上記第 0 行目 R 0 を非選択にして代わって第 1 行目 R 1 を選択状態にする。このようにして、N - 1 行目までの単位回路の読み出しが順次に行われる。真性乱数 R R は、上記単位回路のシリアル出力 R と、1 つ前の出力との排他的論理和により決定される。なお、第 10 図の真性乱数発生回路の動作波形図は、第 9 図と類似しているので省略する。第 9 図と異なる点は、選択信号 R 0 ~ R N - 1 がないことである。それによって N 進カウンタを進行させるための動作が不要となり、M × N 個の単位回路（基本回路）を全て選択するために必要なサイクルが M 回となる。

第 12 図には、この発明に係る真性乱数発生回路の他の一実施例の概念図が示されている。この実施例では、算術方式の乱数発生回路と、本発明にかかる物理現象を利用した真性乱数発生回路を組み合わせた方法によって、乱数を発生させるものである。前述のように算術方式の乱数発生回路は、回路が比較的小規模であるが、得られる乱数の品位は高くない。特に、無数の乱数を取得した場合、周期性が表れるという本質的な欠点がある。そこで、算術方式のアルゴリズム中に、この発明に係る真性乱数発生回路での電気信号ノイズに応答した不規則な要素を初期値

として挿入することで、周期性を低減することが可能である。

第13図には、第12図の初期値発生回路の一実施例の回路図が示されている。この実施例は、基本的には前記第6図の実施例と同様である。異なる点は、排他的論理和 $EX_0 \sim EX_n$ に代えてフリップフロップ回路 $FF_0 \sim FF_n$ が設けられ、かかるフリップフロップ回路 $FF_0 \sim FF_n$ から $D_0 \sim D_n$ のような初期値を得るものである。

上記信号 $D_0 \sim D_n$ は、そのうちの大半が前記のようなプロセスバラツキによって固定値となるが、そのうちのいずれか1ないし数ビットが電気信号ノイズに応答した乱数となるので、上記算術方式乱数発生回路の初期値としての機能を十分に発揮させることができる。

第14図には、第12図の初期値発生回路の他の一実施例の回路図が示されている。この実施例は、基本的には前記第6図の実施例と同様である。異なる点は、活性化信号 ACT によって1ビットの乱数をフリップフロップ回路 FF から出力させるものである。つまり、この実施例では1ビットの乱数を前記算術方式乱数発生回路の初期値としての用いるものである。

第15図には、第13図と第14図の初期値発生回路の動作を説明するための波形図が示されている。動作制御信号 ACT をハイレベルにすると、第13図の回路では各单位回路 $UC_0 \sim UC_n$ から出力信号 $R_0 \sim R_n$ が出力される。この出力信号 $R_0 \sim R_n$ は、前記のように固定値となるものや電気信号ノイズに対応して変化するものが存在する。動作制御信号 ACT をハイレベルからロウレベルにすると、そのときの上記出力信号 $R_0 \sim R_n$ に対応した乱数 $D_0 \sim D_n$ がフリップフロップ回路 $FF_0 \sim FF_n$ に取り込まれて、固定値を含む $D_0 \sim D_n$ からなる複数ビットからなる乱数が出力される。

第14図の回路では、上記各单位回路 $UC_0 \sim UC_n$ の出力信号 R_0

～R_nが排他的論理和回路EX0～EX_nに供給され、そのときどきの信号R₀～R_nに対応した1ビットの乱数が排他的論理和回路EX0～EX_nを通して出力されている。したがって、動作制御信号ACTをハイレベルからロウレベルにすると、そのときに生成されている乱数が
05 フリップフロップ回路FFに取り込まれて、1ビットからなる乱数DMが出力される。

第16図には、この発明に係る真性乱数発生回路の他の一実施例の回路図が示されている。この実施例は、前記第9図に示した真性乱数発生回路に識別情報Fを出力させる出力端子が設けられる。つまり、M×N
10 個の単位回路から出力されるM×N個の出力信号が識別情報Fとして出力される。上記識別情報Fは、適当な記憶回路に保持されて管理システムに登録される。この識別情報Fの照合方法としては、登録時と照合時の環境や条件の違いの他に前記のように電気信号ノイズに応答する真性乱数に対応した識別番号の変動を許容する必要がある。上記真性乱数発生回路を搭載した半導体集積回路装置に電源投入等を行った際、あるい
15 は前記動作活性化信号ACTを活性化した直後の識別信号Fを適当な記憶回路に記憶させて、これを被識別番号とする。管理システムから登録識別番号を順次取り出す。登録識別番号と被識別番号を比較する。

登録識別番号と被識別番号の比較結果の違いが小さいものを一致候補
20 にする。この動作を管理システムに登録されている登録識別番号について繰り返すことで、最終的に全ての登録識別番号の中で最も違いが小さいものが同一最有力候補となる。

登録識別番号と被識別番号を比較において、対応するビットの”0”、”1”出力パターンは、個々の登録識別番号に特有であり、同一の半
25 導体集積回路装置から出力された識別番号であるかは、パターンを構成するビット数の一致の割合で判定できる。登録時と照合時の環境や前記

乱数ビットでの違いによる識別番号の変動を許容するため、被識別番号と登録済みの識別番号とのずれの合計がもつとも小さいものを一致の候補とすることによりチップ識別が可能となる。

第 17 図には、この発明に係る真性乱数発生回路の一実施例の回路図
05 が示されている。この実施例は、基本構成は前記第 9 図の実施例と同様である。本願においては、M O S F E T の特性のバラツキはランダムな分布であることに着目し、数多くの単位回路を観察すれば、第 1 インバータ回路 I N V 1 と第 2 のインバータ回路 I N V 2 又は第 1 ゲート回路 G 1 と第 2 ゲート回路 G 2 の特性が極めて等しい組み合わせがある確率
10 で存在することを利用するものである。このために、半導体集積回路装置に真性乱数発生回路を製造した場合に、実際に電気信号ノイズを反映させる単位回路が存在するか否かの検査を行うことが不可欠となる。

この実施例では、真性乱数発生回路に自身を試験するテスト回路が付加される。このテスト回路での検査方法は、単位回路群中に含まれる第
15 1 ゲート回路 G 1 (第 1 インバータ回路 I N V 1) と第 2 ゲート回路 G 2 (第 2 インバータ回路 I N V 2) の特性が極めて等しい組み合わせの単位回路の数を判定し、物理現象に基づく電気信号ノイズを確実に捉えることを保証するものである。

前記第 16 図において識別情報 F を取り出したように、各単位回路か
20 らの出力信号を得られる回路ノード、つまりはインバータ回路 I N V 1 の出力端子 (排他的論理和回路 E X の一方の入力) の信号 R を反転検出器に供給し、この検出信号 H を計数器により計数する。この計数出力 C を比較器で比較し、判定結果 M を得るものである。また、上記テスト動作のために (4 + M) 進カウンタにより列選択信号を形成するように
25 される。(4 + M) 進カウンタは、同じ単位回路を 4 回連続して選択すると、次の単位回路の選択動作に移るという動作を繰り返して行う。

第 18 図には、上記テスト回路の動作の一例を説明するためのタイミング図が示されている。テスト信号 T S をハイレベルにして (4 + M) 進カウンタ動作を指示する。また、反転検出器と計数器を初期状態又は初期値とする。動作制御信号 A C T をハイレベルにして乱数発生回路を動作状態にする。クロック C L K の供給して最初の単位回路からの順次の読み出し動作を行う。このとき、(4 + M) 進カウンタは、クロック C L K 1 ~ 4 に対して同じ単位回路を 4 回連続して選択する。これにより、前記第 2 図 (b) のように固定値を出力するものは、4 回とも同じ信号 R が出力される。

このように固定値を出力させるものは反転検出器は反転検出を行わないので、計数器の計数値は増加しない。これに対して、第 2 図 (a) のように電気信号ノイズ V n z に応答した出力信号 R を形成するものが存在すると、4 回のアクセス中での反転回数は最大で 3 回であるが、1 回以上の反転した場合には検出結果は真とする。同図では、2 サイクル目と 4 サイクル目で出力信号 R が変化し、このように反転検出器では出力 H のレベルがその都度変化する。

このように 1 回でも出力 H が変化すると、結果が真であるとき計数器の値 C 0 をロウレベルからハイレベルに変化させて計数値を 1 増やす。単位回路群中の次の単位回路の選択に移り、最後の単位回路まで上記同様な検出動作を繰り返して行う。計数器の数が規定値より大きい時、検査結果 M の値を真 (ハイレベル) とする。真性乱数を得る場合には基本的には上記規定値は 1 であればよいが、安全性を考慮して 2 又は 3 以上の複数にすることが望ましい。

例えば、第 18 図に示したように計数器を 2 ビット出力のバイナリカウンタとしたとき、クロック C L K の K - 1 サイクル目で計数出力 C 0 と C 1 が共にハイレベルになることを比較器が検出して上記検査結果 M

をハイレベルのように決めれば、第2図(a)のように電気信号ノイズ V_{nz} に応答した出力信号 R を形成するものが4個以上存在することが確かめられたことになる。

1つの単位回路を検査に対してCLKパルスの4個で4回アクセスしたが、最低2回以上であつても構わない。2回アクセスする時は、(2 + M)進カウンタを用いるものである。検査以外のときには、上記テスト信号TSのロウレベルの応じて前記のようにM進カウンタとして動作するようにされる。あるいは、そのまま(4 + M)進カウンタや(2 + M)進カウンタとして動作させてもよい。この場合には、読み出しサイクルが4倍又は2倍に増加する。

セキュリティ製品における政府機関の規定として、NIST(米国標準技術研究所)が策定したFIPS 140-2がある。この中には、政府の購入品が備える暗号モジュールが満たすべきセキュリティ要件(FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES)が規定されており、乱数については統計的手法による、品位の検定合格基準が示されている。当該方法を用いた方法では、それを実現するための専用の回路の規模が比較的大きいことや、半導体試験装置で検査する場合に比較的時間がかかるという短所がある。

これに対して、この発明に係る乱数発生回路に設けられたテスト回路では、半導体ウェハ上に回路が完成した時点で、上記テスト機能を備えたテストに接続することなく、自身で判定を行うことができる。また、半導体集積回路装置として出荷時にも自身で判定することが可能である。更に、必要ならシステムに搭載された時点で、必要に応じてあるいは定期的に上記真性乱数発生回路が正常に動作可能な状態であるか否かの確認を行うことができる。これによって、信頼性の高い真性乱数発生が可能となるものである。いずれも、本方式が統計に裏付けられたもので

あることにより可能である。

すなわち、真性乱数発生回路の診断（試験）は、その乱数の品位の評価に等しく、ある種の統計的処理が必要である。そのため、試験装置、試験時間、長期信頼度保証などの大きな課題がある。特に、真性乱数発生器がL S I や最終システムに搭載された以降、回路自体が正常に動作しているか重要な問題である。何故なら、品位の高い真性乱数が得られなければ、セキュリティが危ぶまれることになるからである。しかし、真性乱数発生回路を試験あるいはモニタすることは稼働中のシステムとしては大きな負荷である。このような技術的課題に対して、本願発明の真性乱数発生回路では、上記のように簡単な構成でこれらの問題を解決することができる。

第19図には、この発明に係る真性乱数発生回路の一実施例の回路図が示されている。この実施例は、基本構成は前記第9図の実施例と同様である。この実施例では、クロックとして発振器で形成した発振パルスOSCを用いるようにするものである。

第20図には、第19図の真性乱数発生回路の動作波形図が示されている。活性化信号ACTにより、発振器が特定の周期 T_{osc} のパルスを発生する。パルスOSCを受けて、単位回路群中の単位回が順次選択され、RR信号に乱数が生成される。スタート信号STをハイレベルに遷移させると、RR信号の乱数が出力RYから取り出される。スタート信号STの周期 T_c と発振器の周期 T_{osc} の関係は、全ての単位回路からの出力信号の読み出しを必要とするから、 $[T_c] \geq [T_{osc}] \times [n]$ である。ここで、上記の $[n]$ は、単位回路群中の単位回路数（ $M \times N$ ）である。発振器出力パルスOSCは、かかる真性乱数発生回路が搭載されたL S I のシステムクロック等であつてもよい。

第21図には、この発明に係る真性乱数発生回路の一実施例の回路図

が示されている。この実施例は、基本構成は前記第 19 図の実施例と同様である。この実施例では、スタート信号 S T が省略されて、動作制御信号 A C T より動作状態となり、シフトレジスタが出力の直前に設けられて並列ビットからなる乱数 R A i を生成するようにされる。

- 05 第 22 図には、この発明に係る乱数発生回路の出力部の他の一実施例の回路図が示されている。この実施例は、前記第 21 図の実施例のシフトレジスタをメモリに変更している。同図で用いたメモリは、いわゆるシリアル入力／パラレル出力型のメモリである。制御信号 A C T がハイレベルの時、真性乱数発生回路からクロックの $M \times N$ サイクル毎に R R
- 10 から 1 ビットずつ真性乱数発生し、また同時に当該メモリはシリアル入力モードであって、入力 S I から真性乱数を取り込み蓄積する。制御信号がロウレベルの時、真性乱数発生回路は停止し、同時に当該メモリはパラレル出力モードであって、入力 A D のアドレス情報に対応したメモリ空間に蓄積された真性乱数を出力 D T から出力する。なお、当該メモリ
- 15 の各入出力の意味は、S E はこのメモリのモードを切り替えるための制御入力であって、ハイレベルの時シリアル入力モード、ロウレベルの時パラレル出力モードであり、S I はシリアルデータ入力であり、C K はシリアル入力を取り込む時の同期信号入力であり、A D はパラレル出力モードの時メモリ空間を選択するアドレス入力であり、D T はパラレル
- 20 データ出力である。

第 22 図に示されたメモリは、F I F O (First In First Out) 型メモリや、シリアル入力とパラレル出力を同時に行える非同期型メモリであっても構わない。

- 第 23 図には、前記第 21 図に示した真性乱数発生回路の動作波形図
- 25 が示されている。動作制御信号 A C T により回路が動作状態となり、N 進カウンタのキャリー信号 C A によってシフトレジスタが 1 ビットのシ

フト動作を行い生成された真性乱数RRの取り込みを行う。この実施例では、0ないし7からなる8回の前単位回路群の読み出しによって、8ビットからなる乱数D0～D7をパラレルに出力させることができる。

第24図には、この発明に係る真性乱数発生回路の一実施例のチップ構成図が示されている。この実施例では、真性乱数発生回路を1つのICで構成するものである。外部端子として電源端子VCC、VSS、クロック入力端子CLK、動作制御信号RST及び真性乱数出力端子RRから構成される。前記のように発振器を搭載したものでは、クロック端子CLKが省略される。また、テスト回路を備えたものでは、判定出力端子、テストモード入力端子等が付加される。判定出力端子は、乱数出力端子RRと許容することもできる。かかるICチップを1つのパッケージに封止しても、他のICと同じ実装基板に搭載して封止（マルチチップIC）しても、また、そのままシステムに実装しても構わない。

第25図には、この発明に係る半導体集積回路装置の一実施例のブロック図が示されている。この実施例の各回路ブロックは、実際の半導体基板上における幾何学的な回路配置に合わせて描かれている。この実施例の半導体集積回路装置は、特に制限されないが、複数の回路機能ブロックが組み合わされて特定の信号処理機能を持つようにされる。このような回路ブロックを有する半導体集積回路装置に真性乱数発生回路が搭載される。真性乱数発生回路に必要とされるクロックは、かかる半導体集積回路装置に設けられたクロック発生回路で形成されたクロック又は外部端子からクロック供給を受けるものではそのクロックが用いられる。また、第19図や第21図の乱数発生回路のように発振器を持つものでは、上記のようなクロックの供給は不要である。

第26図には、この発明に係る半導体集積回路装置の他の一実施例のブロック図が示されている。この実施例の各回路ブロックも、実際の半

- 導体基板上における幾何学的な回路配置に合わせて描かれている。この実施例は、MPU（マイクロプロセッシングユニット）を中心とした1チップのマイクロコンピュータに向けられている。このマイクロコンピュータでは、バスBUS（アドレスバス、データバス及びコントロールバス）上に上記MPUの他に、RAM（ランダム・アクセス・メモリ）、ROM（リード・オンリー・メモリ）、DMAC（ダイレクト・メモリ・アクセス・コントローラ）、TIM（タイマー）及びADC（アナログ・デジタル・コンバータ）、DAC（デジタル・アナログ・コンバータ）と、この前記の真性乱数発生回路が接続される。
- 10 本発明に係る真性乱数発生回路は、全て標準CMOS論理回路のみで実現される。このことは、複雑なアナログ回路設計やLSI実装に掛かる負荷を軽減し、製品の価格を低減し、信頼性の向上に寄与することになる。また、セキュリティ問題において最大の課題である、クラッキングに対して強固なモジュールを提供できる。何故なら、標準論理回路
- 15 のみで構成することで、LSIの中でアタックの標的から逃れる、迷彩（ステルス）効果が得られるからである。つまり、アナログ回路を用い場合のように回路パターンに特徴がなく、しかも上記のようにバスBUSを介して乱数の取り出しを行うようにした場合には、上記迷彩（ステルス）効果をいっそう高くすることができる。
- 20 第27図には、この発明に係る真性乱数発生回路の他の一実施例の構成図が示されている。第27図（a）には、回路ブロック構成が示され、第27図（b）には、レイアウト構成が示されている。この実施例では、例えば前記第7図に示したような真性乱数発生回路が n 個設けられる。つまり、0ないし $n-1$ からなる n 個の真性乱数発生回路が設けられ、それぞれの出力信号 R_0 、 $R_1 \sim R_{n-1}$ はマルチプレクサMUX
- 25 を通して1つつの信号が選ばれて真性乱数 R_M として出力される。

第27図(b)のレイアウト構成に示すように、マルチプレクサを挟んで上下に真性乱数発生回路を設けることにより、効率よく回路配置を行うことができる。同図において、真性乱数発生回路の中の1つの回路ブロックは、例えば前記1つの単位回路を表している。この構成において、2つの真性乱数発生回路に挟まれたマルチプレクサは2つのうちの1つを選択するというような比較的簡単な構成で良いから、マルチプレクサが配置される部分には前記デコーダ等の選択信号発生回路が配置される。

例えば、この実施例の真性乱数発生回路において乱数Rを得るのにn個の単位回路で構成される場合、1ビットの乱数Rを得るためには前記のように全ての単位回路からの出力信号を得る必要からにnサイクルを費やすことになる。そこで、上記1つの乱数を得るに必要なnサイクルに対応してこの実施例のようにn個の乱数発生回路を設けた場合には、クロックCLKに同期した高い周波数で乱数を発生させることができる。ただし、動作制御信号により動作を開始したときからnサイクルからなるダミーサイクルを必要とする。

第28図には、第27図に示した真性乱数発生回路の動作の一例を示すタイミング図が示されている。第27図の真性乱数発生回路では、最初の乱数発生回路の読み出しのためにnサイクル(nクロック)後から各真性乱数発生回路から乱数 $R_0 \sim R_{n-1}$ が出力されるから、マルチプレクサMPXによりクロックCLKに同期して1個ずつ選ぶようすることにより、クロックCLKに同期した真性乱数 R_M (R_0 、 R_1 、 $R_2 \cdots R_{n-1}$ 、 R_0' 、 R_1' 、 R_2' 、 \cdots)のようにクロックCLKに同期した高ビットレートな真性乱数を得ることができる。

第29図には、この発明が適用されるICカードの一実施例の外観図が示されている。ICカードは、プラスチックケースからなるカード1

0 1 と、かかるカード 1 0 1 の内部に搭載された図示しない 1 チップのマイクロコンピュータ等からなる IC カード用チップを持つものである。上記 IC カードは、さらに上記 IC カード用チップの外部端子に接続されている複数の接点（電極） 1 0 2 を持つ。

- 05 複数の接点 1 0 2 は、後で第 3 0 図によって説明するような電源端子 V C C、電源基準電位端子 V S S、リセット入力端子 R E S バー、クロック端子 C L K、データ端子 I / O - 1 / I R Q バー、I / O - 2 / I R Q バーとされる。IC カードは、かかる接点 1 0 2 を通して図示しないリーダーライタのような外部結合装置から電源供給を受け、また外部
- 10 結合装置との間でのデータの通信を行う。

- 第 3 0 図には、この発明に係る IC カードに搭載される IC カード用チップ（マイクロコンピュータ）の一実施例の概略ブロック図が示されている。同図の各回路ブロックは、公知の M O S 集積回路の製造技術により、特に制限されないが、単結晶シリコンのような 1 個の半導体基板
- 15 上において形成される。

- この発明に係る IC カード用チップの構成は、基本的にマイクロコンピュータと同じような構成である。その構成は、クロック生成回路、中央処理装置（以下、単に C P U という）、R O M (Read Only Memory) や R A M (Random Access Memory)、不揮発性メモリ（E E P R O M）などの記憶装置、暗号化及び復号化処理の演算を行なうコプロセッサ（暗号化・復号化装置）、入出力ポート（I / O ポート）などからなる。
- 20

- クロック生成回路は、図示しないリーダーライタ（外部結合装置）から第 2 9 図の接点 1 0 2 を介して供給される外部クロック C L K を受け、かかる外部クロック信号に同期したシステムクロック信号を形成し、そ
- 25 れをチップ内部に供給する回路である。

C P U は、論理演算や算術演算などを行う装置であり、システムコン

トロールロジック、乱数発生器及びセキュリロジック及びタイマなどを制御する。RAM、ROM、EEPROMのような記憶装置は、プログラムやデータを格納する装置である。コプロセッサは、DES暗号法などに適合された回路から構成される。I/O（入出力）ポートは、リーダライタと通信を行う装置である。データバスとアドレスバスは、各装置を相互に接続するバスである。

上記記憶装置のうち、ROMは、記憶内容が不揮発的に固定されているメモリであり、主にプログラムを格納するメモリである。揮発性メモリ（以下、RAMという）は自由に記憶情報の書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消えてなくなる。ICカードがリーダライタから抜かれると電源の供給が中断されるため、上記RAMの内容は、保持されなくなる。

上記不揮発性メモリ（以下、EEPROM(Electrical Erasable Programmable Read Only Memory)という）は、内容の書き換えが可能な不揮発性メモリであり、その中に一旦書き込まれた情報は、電源の供給が停止されてもその内部に保持される。このEEPROMは、書き換える必要があり、かつICカードがリーダライタから抜かれても保持すべきデータを格納するために使われる。例えば、ICカードがプリペイドカードとして使用されるような場合、のプリペイドの度数などは、使用するたびに書き換えられる。この場合の度数などは、リーダライタが抜かれてもICカード内で記憶保持する必要があるため、EEPROMで保持される。

CPUは、いわゆるマイクロプロセッサと同様な構成にされる。すなわち、その詳細を図示しないけれども、その内部に命令レジスタ、命令レジスタに書込まれた命令をデコードし、各種のマイクロ命令ないしは制御信号を形成するマイクロ命令ROM、演算回路、汎用レジスタ（R

G 6 等)、内部バスBUSに結合するバスドライバ、バスレシーバなどの入出力回路を持つ。CPUは、ROMなどに格納されている命令を読み出し、その命令に対応する動作を行う。CPUは、I/Oポートを介して入力される外部データの取り込み、ROMからの命令や命令実行のために必要となる固定データのようなデータの読み出し、RAMやEEPROMに対するデータの書き込みと読み出し動作制御等を行う。

上記CPUは、クロック生成回路から発生されるシステムクロック信号を受けそのシステムクロック信号によって決められる動作タイミング、周期をもって動作される。CPUは、その内部の主要部がPチャンネル型MOSFETとNチャンネル型MOSFETとからなるCMOS回路から構成される。特に制限されないが、CPUは、CMOSスタティックフリップフロップのようなスタティック動作可能なCMOSスタティック回路と、信号出力ノードへの電荷のプリチャージと信号出力ノードへの信号出力とをシステムクロック信号に同期して行うようなCMOSダイナミック回路とを含む。

コプロセッサは、内部で扱う平文データに符号ビットを付加し、ポジ／ネガの両方の状態を持つようにする。暗号化における繰り返し演算時に、データを符号ごとランダムに変更する。符号の影響を受けない演算（排他的論理和など）はそのまま符号を無視して演算する。符号の影響を受ける演算（変換表を用いた演算など）では、ポジ用の演算回路とネガ用の演算回路を用意し、データの符号によって演算回路の出力を選択する機構を用いる。

DES (Data Encryption Standard) は、広範に用いられている秘密鍵ブロック暗号である。DESのアルゴリズムは、大きく平文のデータフローと鍵のデータフローに分割できる。平文データフローでは、IPとよばれる転置（信号の入れ換え）を行った後、上位と下位それぞれ3

2 ビットずつにデータを分割し、転置・換字処理を 16 回繰り返す。最後に上位と下位それぞれ 32 ビットデータを統合し、 IP^{-1} とよばれる転置を行い、暗号文を得る。

DES では、暗号化と復号化が同じ処理で実現できる。ただし暗号化
05 と復号化では、鍵のスケジューリングが異なる。鍵のスケジューリング部分について、詳細は省略するが、鍵データを元に、各段に対して 48 ビット鍵スケジューリングデータの出力を行う。

DES アルゴリズムでは、同じ平文に対しては常に同じ内部動作を行う。その結果、内部信号が入力信号に依存して変化するので、DPA (D
10 iffrential Power Analysis) 法での統計処理を行いやすい。つまり、DPA 法では、消費電流波形を統計処理して暗号鍵を推定し、例えば DES のある部分に仮定した暗号鍵を当てはめて、平文を変化させながら消費電流波形を測定して統計する。暗号鍵を様々に変化させながらこの作業を繰り返し、正しい鍵のときには電流波形が大きなピークを示す。

15 上記のような DPA による DES 解読に対する対策の例として、特開 2000-066585 号公報がある。この公報に記載の技術では、マスク a のパターンと、そのビット反転のマスクパターンのペアを設け、暗号化を行う毎にこのペアの一方をスイッチによりランダムに選択して、装置内部の平文に依存したビットをマスクし、暗号文を出力する前に
20 暗号文からマスク a の影響を除去するようにするものである。

DPA による解読防止のためには、上記マスクが特定のパターンに偏らないようにする必要のあることは説明されているが、どのようにすれば複数ビットのパターンが偏らないようにするために、乱数発生器で生成された乱数が利用される。

25 第 31 図には、この発明が適用される非接触 IC カードの一実施例のブロック図が示されている。同図には、非接触 IC カードに対して、外

部装置として設けられるリード・ライト装置のコイル（アンテナ）も併記されている。非接触 I C カードに搭載される L S I は、図示されるブロックの他に、例えばメモリやマイクロコンピュータ等の機能ブロックを備えるが、それらを論理回路及び不揮発メモリとして表している。上
05 記 L S I の各ブロックを構成する回路素子は、特に制限されないが、公知の M O S F E T（金属酸化物半導体型電界効果トランジスタ。この明細書では、M O S F E T をして絶縁ゲート型電界効果トランジスタの総称とする）集積回路の製造技術により、単結晶シリコンのような 1 個の半導体基板面上に形成される。また、この L S I は、所定の保護膜によ
10 ってラミネート処理された後、非接触 I C カードの基体となるカード面上に搭載され、さらに被膜処理が施される。

本実施例の非接触 I C カードは、特に制限されないが、いわゆる密着型の非接触 I C カードとされ、例えば銅箔等を用いてカード面上にコイル状に形成される受電コイル（カード側アンテナ）と、所定の配線層を
15 介して上記受電コイルに結合される L S I とを備える。この L S I は、4 個のダイオードがブリッジ結合されてなる整流回路と、整流回路の整流電圧を平滑する平滑コンデンサと、安定化電源回路とによって、上記論理回路及び不揮発メモリ等を含む内部回路の動作電圧 V D D が形成される。上記整流回路に対しては、実質並列形態にクロック発生回路、デ
20 ータ受信回路及びデータ送信回路が設けられる。

上記ダイオードブリッジ回路からなる整流回路は、リード・ライト装置の送電コイル（アンテナ）との電磁結合によって非接触 I C カードの受電コイルに電力源として伝達される交流信号つまりキャリアを整流し、
上記平滑コンデンサで平滑した電圧を安定化電源により直流電源電圧 V
25 D D を生成し、L S I の各機能ブロックに動作電源として供給する。パワーオンリセット回路は、電源電圧 V D D の立ち上がりを検知し、つま

りは、リード・ライト装置との結合を検知して、データの受信や送信を正常に行うようにするために、論理回路のレジスタやラッチ回路等をリセットさせる。

05 データ受信回路は、リード・ライト装置から例えばキャリアを周波数変調することにより伝送されるデータを受信復調し、内部入力データとしてL S I の内部回路に伝達する。内部回路で形成された出力データは、データ送信回路によりキャリアを周波数変調してリード・ライト装置に伝送する。

10 上記のような内部回路（論理回路）やデータ受信回路及びデータ送信回路では、上記動作電圧V D Dの他に、動作シーケンス制御や信号の受信や送信のためにクロック信号を必要とする。この実施例では、クロック発生回路により上記交流信号をパルス信号とし、クロック信号を生成する。論理回路部には、乱数発生器が設けられており、外部とのデータ送信やデータ受信にかかる乱数が用いられる。

15 上記非接触 I C カードでは、直流電源電圧V D Dの電流供給能力が小さいから、乱数発生器における消費電力も小さいことが必要とされる。前記のよう乱数発生器は、単位回路を順次に動作させるものであるために消費電流を小さくできる。それ故、この実施例の乱数発生器は、上記のような非接触 I C に搭載させるものとして好適なものとなる。

20 第 3 2 図には、この発明に係る乱数発生回路で生成された乱数の乱数 2 次元散布図が示されている。同図においては、2 0 0 × 2 0 0 ビットの乱数の 0 と 1 をドットの白と黒に対応して表示したものである。特に制限されないが、この実施例では、単位回路（基本回路）を 1 2 8 個設けて、通常の C M O S プロセスで回路を構成したものである。

25 同図は、図面の作成の関係で乱数 2 次元散布図を 4 0 0 d p i でスキャナーで読み取り表示したものであるので、実際の乱数 2 次元散布図と

は若干異なるが、おおよその乱数 2 次元散布を表しており、特有のパターンは存在しないことが判る。つまり、高い品位の乱数であることを表している。また、前記の F I P S 1 4 0 - 2 での乱数検定結果は、次の通りである。1 回の検定に使用される乱数の長さを 2 0 , 0 0 0 ビット
05 とし、これを 6 0 0 回行った結果、全てにおいてかかる検定をパスすることができた。

今日暗号やセキュリティが日常的に話題となるようになったのは、インターネットの普及が理由であろう。インターネットは遠く離れた機器をつなぐネットワーク技術である。インターネット上を往来するデータ
10 は、本質的に第三者の所有するコンピュータやネットワーク装置を通過するため盗聴や改竄の虞が常にある。インターネットをセキュリティやプライバシーが保証された安全なインフラとするために、暗号や認証が脚光を浴びている。現在、インターネット上で様々なセキュリティ技術が利用されているが、その代表的なものに S S L (Secure Socket Layer)
15 r) や I P s e c (Internet Protocol security) 技術などがある。これらの技術の詳細は記さないけれども、いずれも品位の高い乱数が必要である。特に、I P s e c は次世代のインターネット技術である I P v 6 (Internet Protocol Version6) では必須条件として採用される。I P v 6 は普及すると、個人の持つパーソナルコンピュータや携帯電話を
20 はじめ、自動車や家電製品などにも I P 番号が割り当てらことも可能となる。そうすると、品位の高い乱数、つまり真性乱数をそれらの機器の中で容易に生成することが必要となる。

前述のように、本発明に係る真性乱数発生回路は、全て標準 C M O S 論理回路のみで実現される。このことは、複雑なアナログ回路設計や L
25 S I 実装に掛かる負荷を軽減し、製品の価格を低減し、信頼性の向上に寄与することになる。

第 3 4 図には、この発明に係る半導体集積回路装置に搭載される真性乱数発生回路の第 1 図に示された基本概念の応用概念の回路図が示されている。第 1 図では、真性乱数は複数からなる各基本回路内の I N V 1 と I N V 2 に生じる電気信号ノイズを素にしているが、第 3 4 図では、
05 第 1 のインバータ I N V 1 を共通とし第 2 のインバータを各基本回路に分散させる。つまり、1 種類しか存在しない第 1 のインバータの論理しきい値 V L T 1 と各基本回路内の第 2 のインバータの論理しきい値 V L T 2 の差が極めて小さい組み合わせが存在する場合、第 1 のインバータおよび第 2 のインバータの電気信号ノイズの影響を反映して真性乱数を
10 得ることができる。なお、第 3 のインバータ以後の動作は上記第 1 図で述べた内容と同じであるので省略する。

第 3 5 図には、この発明に係る半導体集積回路装置に搭載される真性乱数発生回路の第 3 4 図に示された応用基本概念のさらに別の応用概念の回路図が示されている。この実施例では、前記図 3 4 のインバータ回路 I N V 1 ~ I N V 1 4 が、2 入力のナンド (NAND) ゲート回路 G
15 1 ~ G 1 4 に置き換えられる。上記ゲート回路 G 1 は、一方の入力と出力とが結合される。このゲート回路 G 1 の共通化された入出力が基本回路内のゲート回路 G 0 2 の一方の入力と接続される。ゲート回路 G 0 2 の出力はゲート回路 G 0 3 の一方の入力に接続される。ゲート回路 G 0
20 3 の出力はゲート回路 G 0 4 の一方の入力に接続される。そして、これらのゲート回路 G 0 2 ~ G 0 4 の他方の入力には、電源 V D D に接続され常にハイレベル (論理 1) とさる。

第 3 4 図のインバータ回路 I N V 1 ~ I N V 1 4 は、上記ナンドゲート回路 G 1 ~ G 1 4 のような論理ゲート回路の一種と見做すことができる。すなわち、入力信号を反転させる論理動作を行うものであるからで
25 ある。第 3 4 図のようにインバータ回路 I N V 1 ~ I N V 1 4 を用いた

場合には、インバータ回路 I N V 1 と I N V 0 2 のように初段側においては論理しきい値電圧 V L T 付近で動作するものであり、電源電圧 V D D と回路の接地電位との間に直流電流を流すものとなる。本願発明では、前記のように素子のプロセスバラツキによる論理しきい値電圧の正規分布を利用するものであり、そのために比較的多数からなる単位回路を動作させる必要があるので、上記インバータ回路 I N V 1 と I N V 0 2 での直流電流は低消費電力化を実現する上では無視できない。

これに対して、この実施例のようにゲート回路 G 1 ~ G 1 4 を用いた場合には、各ゲート回路 G 1 ~ G 1 4 は、動作制御信号 A C T をロウレベル（論理 0）のような非活性化レベルとしたとき、ゲート回路 G 1 の出力は無条件にハイレベル（論理 1）となり、例えばゲート回路 G 1 の出力を入力とするゲート回路 G 0 2 の出力は無条件にロウレベル（論理 0）となり、ゲート回路 G 0 2 の出力を入力とするゲート回路 G 0 3 の出力は無条件にハイレベル（論理 1）となり、ゲート回路 G 0 3 の出力を入力とするゲート回路 G 0 4 の出力は無条件にハイレベル（論理 1）となり、各ゲート回路 G 1, G 0 2、G 0 3、G 0 4 およびそれと等価な他の基本回路ないのゲート回路においても直流電流が発生しない。すなわち、この実施例回路では、乱数を必要とするタイミングで上記動作制御信号 A C T をハイレベル（論理 1）のような活性化レベルとする。これにより、各ゲート回路 G 1 ~ G 1 4 は、上記動作制御信号 A C T とは異なる他方の入力信号に応答して反転信号を形成するというインバータ回路としての動作を行う。これにより、上記動作制御信号 A C T をハイレベルにすることにより、第 3 4 図の基本回路図と同様の動作を行うものとなる。

以上本発明者よりなされた発明を実施例に基づき具体的に説明したが、本願発明は前記実施例に限定されるものではなく、その要旨を逸脱し

- ない範囲で種々変更可能であることはいうまでもない。例えば、抵抗素子を、インバータやゲート回路を構成する信号入力MOSFETに対する負荷素子とするような場合には、特性バラツキに応ずる情報は、抵抗素子の特性バラツキと信号入力MOSFETの特性バラツキとの両方を
- 05 反映したものとなる。抵抗バラツキに対応する特定情報は、必ずしも半導体集積回路装置内のみで形成する必要は無く、外部端子を介して接続する構成とすることもできる。ただし、低消費電力化を図る上では、前記のようなCMOSゲート回路を用いることが望ましい。また、第1インバータ回路INV1と第2インバータ回路INV2は、その消費電流
- 10 を低減させるために前記第10図(b)に示したようなクロックドインバータ回路CNに置き換え、動作制御信号により活性化を行うようにするものであってもよい。

産業上の利用可能性

- 15 この発明は、ネットワーク機器に組込むもの、無線通信機器に組み込むもの、暗号化・複合化装置に組み込むもの、認証システムに組み込むもの、あるいは玩具系ロボットやゲームのキャラクタの「個性因子」や「気まぐれ因子」に組み込まれる乱数の乱数発生方法と半導体集積回路装置に広く利用することができる。

20

請 求 の 範 囲

1. 互いに同じ製造過程をもって同一の形態として形成された第1及び第2論理回路と、上記第1論理回路及び第2論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して2値信号を形成する増幅回路とからなる単位回路の複数個と、

05 上記複数個の単位回路から出力される複数個からなる2値信号のうちのいずれか1つの信号変化に応答して出力信号を形成する信号変化検出回路とを用い、

上記信号変化検出回路から出力される2値信号の複数個を組み合わせ

10 て乱数を生成してなることを特徴とする乱数発生方法。

2. 請求の範囲第1項において、

上記第1及び第2論理回路と上記増幅回路とは、第1と第2の入力を有する論理ゲート回路からなり、

上記第1論理回路に対応した論理ゲート回路の第1の入力と出力とが

15 接続され、

上記第2論理回路に対応した論理ゲート回路の第1の入力は、上記第1論理回路に対応した論理ゲート回路の共通接続された入力と出力に接続され、

上記増幅回路は、複数個の論理ゲート回路の第1の入力と出力とが縦

20 列形態に接続され、

上記第1論理回路、第2論理回路及び増幅回路を構成する論理ゲートの第2の入力には上記動作制御信号を供給して上記複数の単位回路を動作状態にして、上記信号変化検出回路を通して乱数を生成してなることを特徴とする乱数発生方法。

25 3. 請求の範囲第2項において、

上記複数の単位回路を順序回路により形成された動作制御信号に対応

して順次に選択状態し、全ての単位回路の出力信号をシリアルに出力させて上記信号変化検出回路により 1 ビット分の乱数を生成してなることを特徴とする乱数発生方法。

4. 請求の範囲第 3 項において、

- 05 上記信号変化検出回路は、上記順序回路よりシリアルに出力される出力信号と 1 つ前に出力された出力信号とを受けて上記乱数を形成する排他的論理回路を用いるものであることを特徴とする乱数発生方法。

5. 請求の範囲第 3 項において、

- 10 上記 1 ビットの乱数に対応した全ての単位回路の出力信号は、チップ識別信号としても利用されるものであることを特徴とする乱数発生方法。

6. 請求の範囲第 1 項において、

上記信号変化検出回路により形成された乱数は、算術方式の乱数発生回路の初期値として用いられ、

- 15 上記算術方式の乱数発生回路より乱数が生成されるものであることを特徴とする乱数発生方法。

7. 互いに同じ製造過程をもって同一の形態として形成された第 1 及び第 2 論理回路と、上記第 1 論理回路及び第 2 論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して 2 値信号を形成する増幅回路とからなる単位回路の複数個から出力される複数ビットからなる信号を初期値として算術方式の乱数発生回路に伝え、

- 20 上記算術方式の乱数発生回路より乱数を生成してなることを特徴とする乱数発生方法。

- 25 8. 互いに同じ製造過程をもって同一の形態として形成された第 1 及び第 2 論理回路と、上記第 1 論理回路及び第 2 論理回路のしきい値電圧の差電圧に重畳される雑音を増幅して 2 値信号を形成する増幅回路とから

なる単位回路の複数個と、

上記複数個の単位回路から出力される複数個からなる 2 値信号のうちのいずれか 1 つの信号変化に応答して出力信号を形成する信号変化検出回路とを備え、

- 05 上記信号変化検出回路から出力される 2 値信号から乱数を生成してなることを特徴とする半導体集積回路装置。

9. 請求の範囲第 8 項において、

上記第 1 及び第 2 論理回路と上記増幅回路とは、第 1 と第 2 の入力とを有する論理ゲート回路からなり、

- 10 上記第 1 論理回路に対応した論理ゲート回路の第 1 の入力と出力とが接続され、

上記第 2 論理回路に対応した論理ゲート回路の第 1 の入力は、上記第 1 論理回路に対応した論理ゲート回路の共通接続された入力と出力に接続され、

- 15 上記第 1 及び第 2 論理回路に対応した論理ゲート回路の第 2 の入力には、動作制御信号が供給されてなり、

上記増幅回路は、複数個の論理ゲート回路の第 1 の入力と出力とが縦列形態に接続され、第 2 の入力には上記動作制御信号が供給されてなることを特徴とする半導体集積回路装置。

- 20 10. 請求の範囲第 9 項において、

上記複数の単位回路は、順序回路により形成された動作制御信号に対応して順次に選択状態にされ、

上記複数の単位回路の出力部には、上記信号変化検出回路が設けられてなることを特徴とする半導体集積回路装置。

- 25 11. 請求の範囲第 10 項において、

上記信号変化検出回路は、上記順序回路より出力される出力信号と 1

つ前に出力された出力信号とを受けて上記乱数を形成する排他的論理回路を含むものであることを特徴とする半導体集積回路装置。

12. 請求の範囲第11項において、

05 上記論理ゲート回路は、CMOS構成の論理ゲート回路であり、上記動作制御信号により単位回路が非動作状態にされるときに、次段のゲート回路のPチャンネルMOSFETをオフ状態にさせるものであることを特徴とする半導体集積回路装置。

13. 請求の範囲第11項において、

10 上記複数の単位回路は、行列配置されてなり、行列配置される各単位回路の入力部には、第1入力と第2入力を有する論理ゲート回路が設けられて、第1入力と第2入力に行及び列選択信号が供給され、その出力により上記第1論理回路及び第2論理回路を構成する論理ゲート回路を選択状態にさせる動作制御信号が形成され、

15 上記各単位回路の増幅回路を構成する論理ゲート回路の第2の入力には、行方向に配置される前段からの単位回路の出力信号が伝えられるものであり、かかる増幅回路は上記動作制御信号が非選択状態のときに前段からの単位回路の出力信号を増幅して伝えるものであることを特徴とする半導体集積回路装置。

14. 請求の範囲第13項において、

20 上記単位回路を構成するMOSFETのゲート長及びゲート幅は、上記信号変化検出回路又は順序回路を含む他の論理回路を構成するMOSFETのゲート長及びゲート幅よりも大きく形成されてなることを特徴とする半導体集積回路装置。

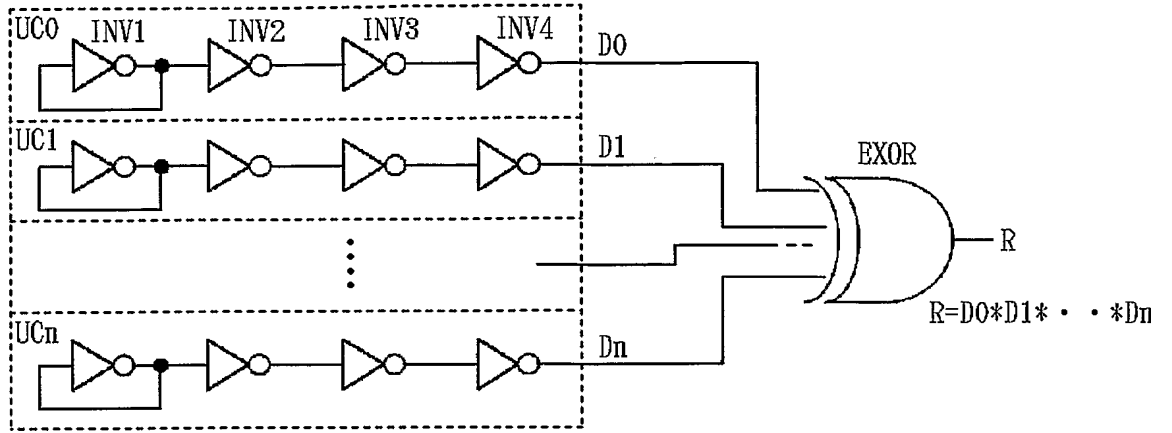
15. 請求の範囲第11項において、

25 上記順序回路は、同じ単位回路を複数回連続して選択するテストモードを備え、

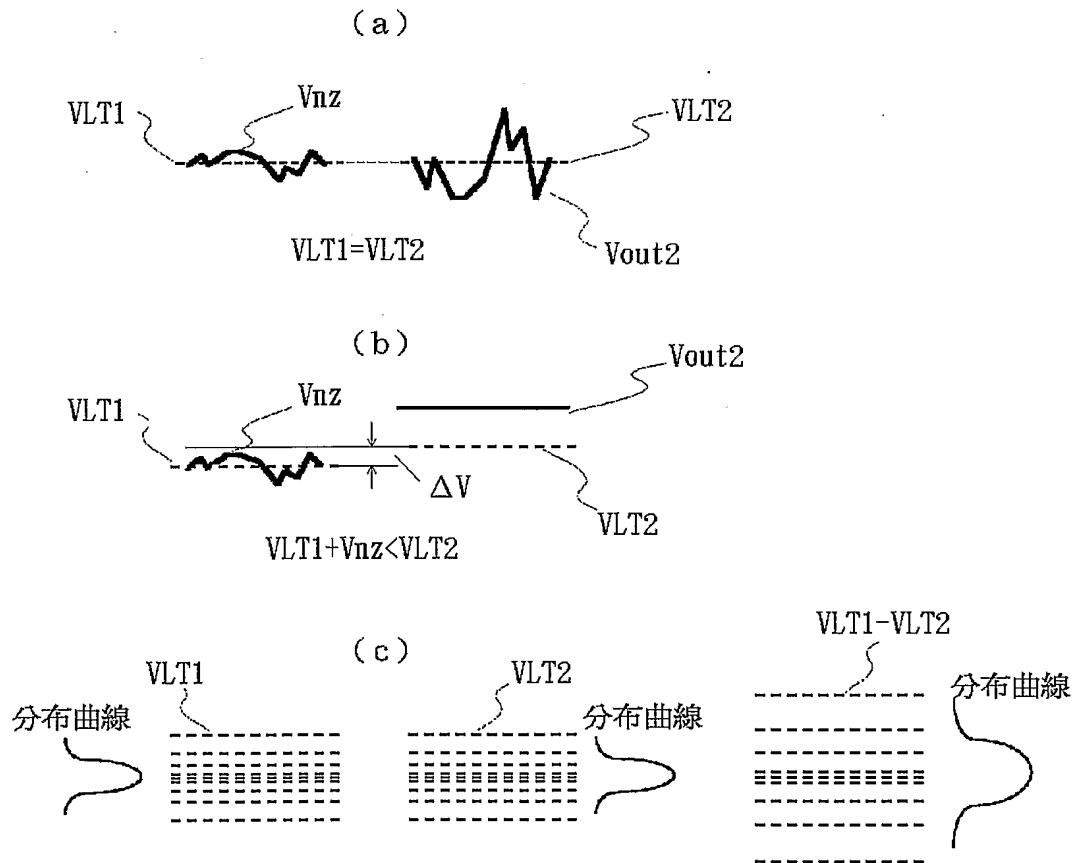
かかるテストモードにおいて、同じ単位回路から複数回出力される出力信号のうち異なる出力を形成する単位回路の数を計数する回路を設け、上記異なる出力信号を形成する単位回路の数が1以上であるときには乱数発生回路は良品として判定してなることを特徴とする半導体集積回路装置。

05

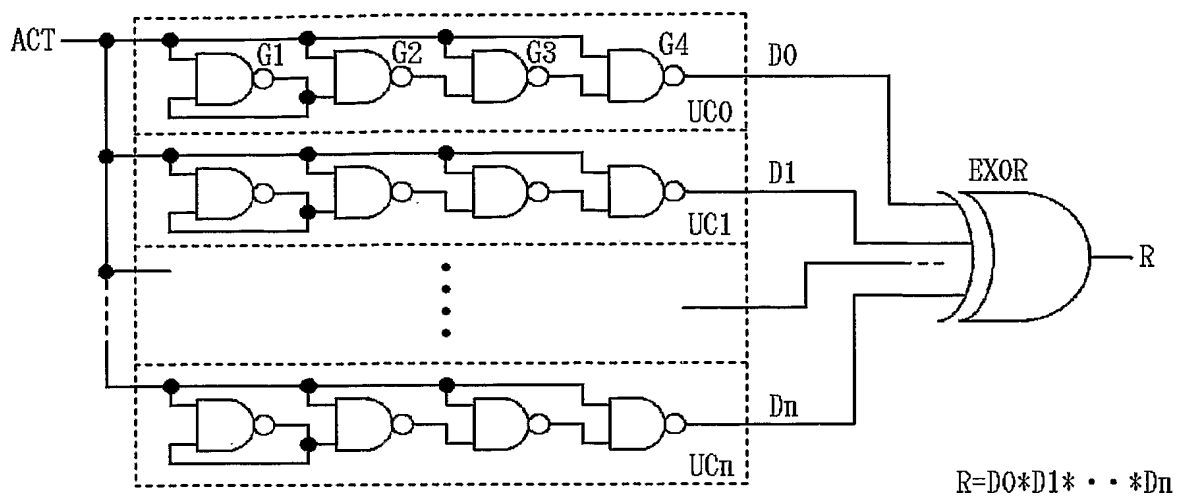
第 1 図



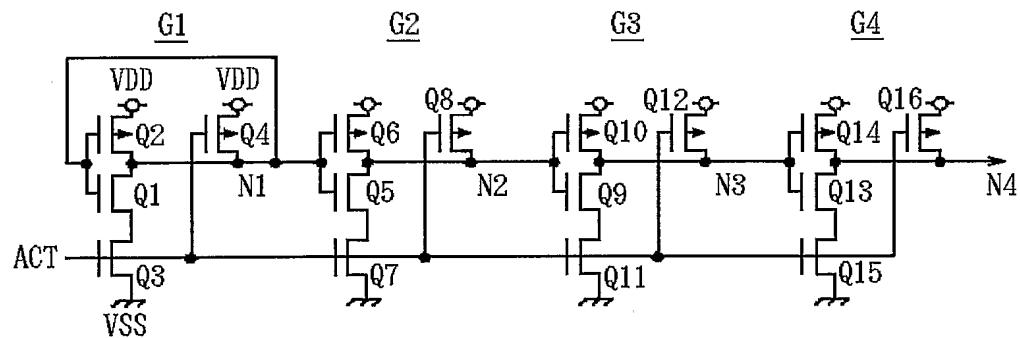
第 2 図



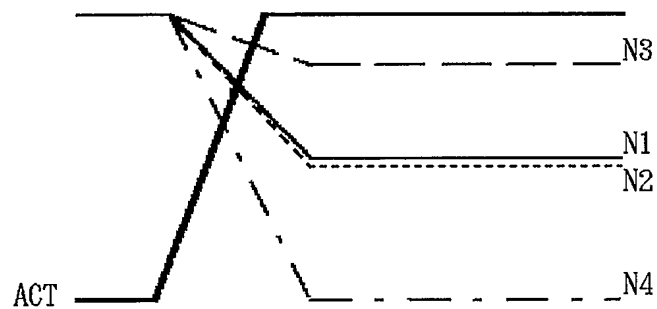
第 3 図



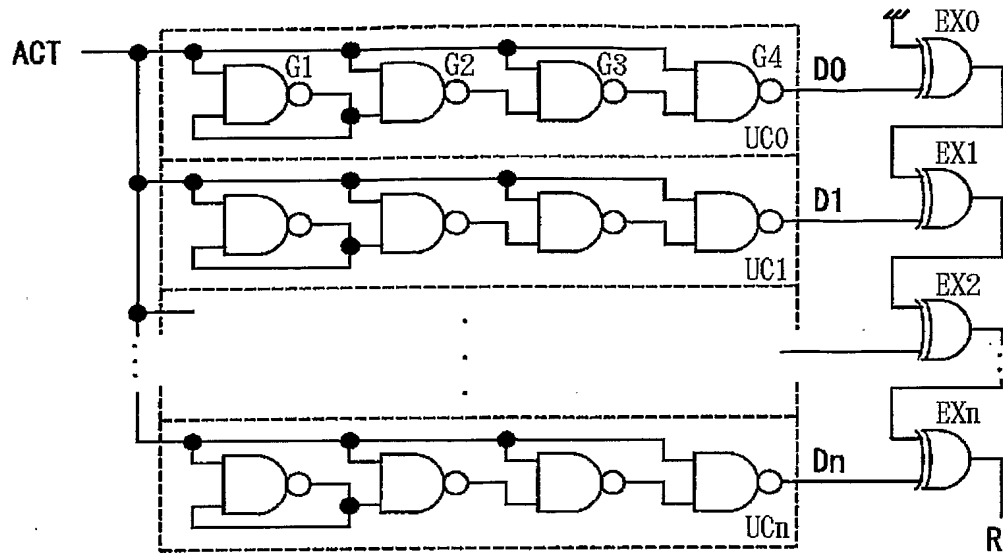
第 4 図



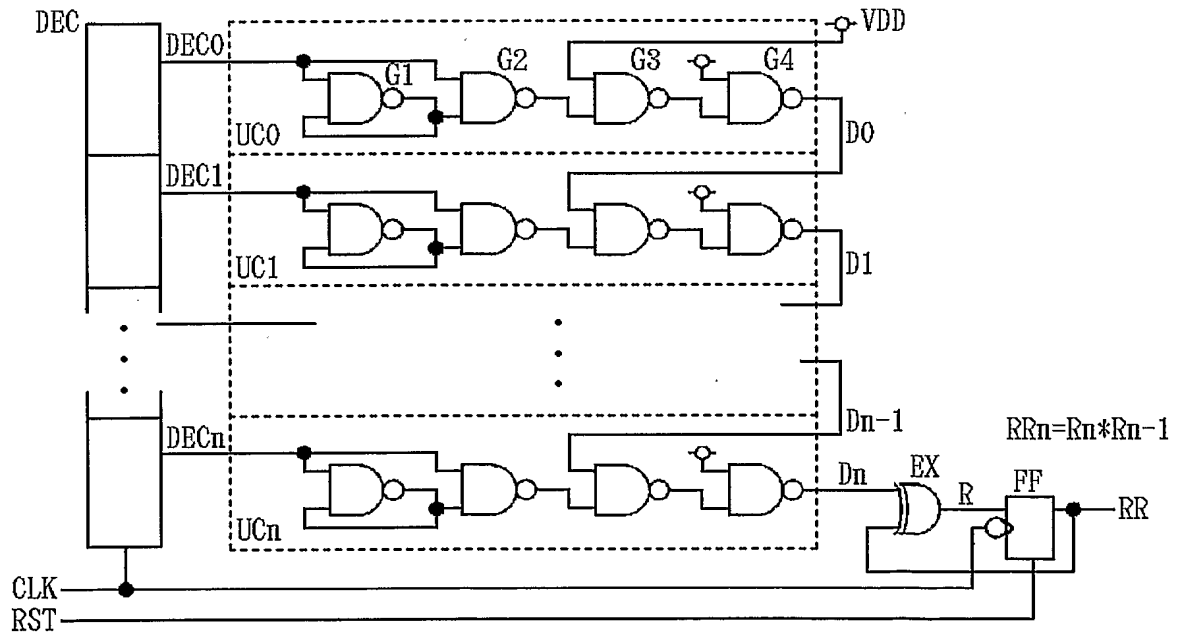
第 5 図



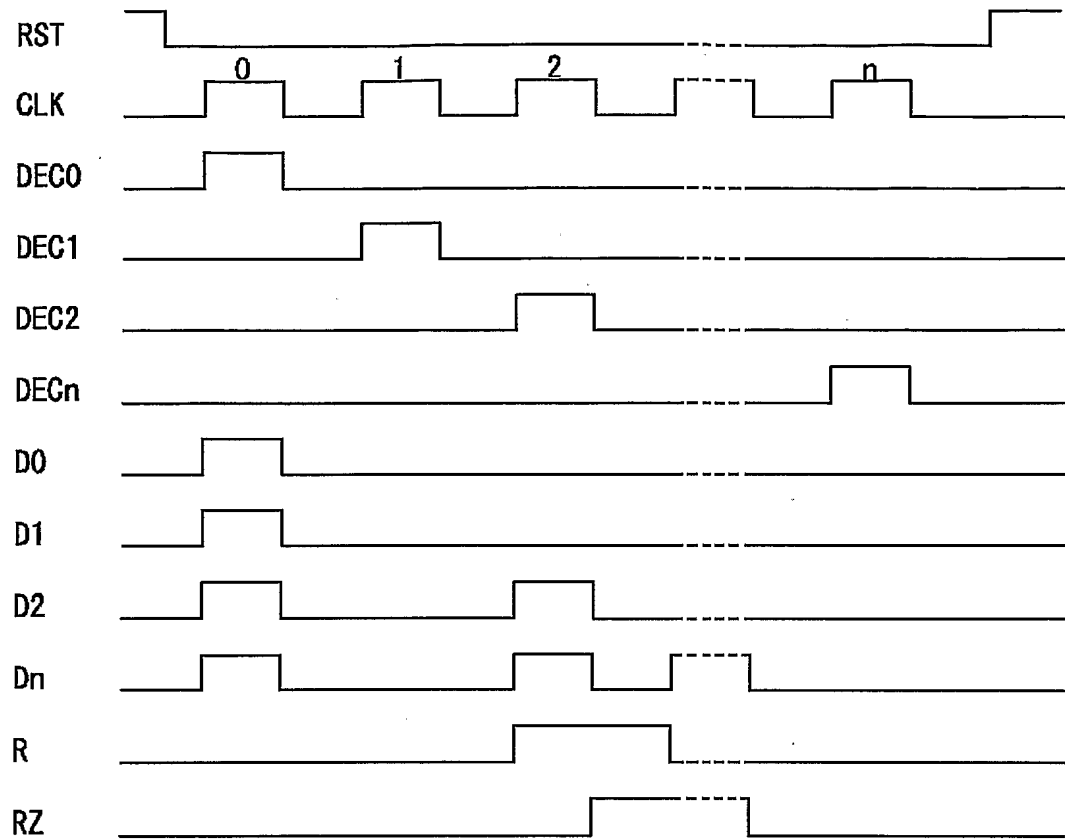
第 6 图



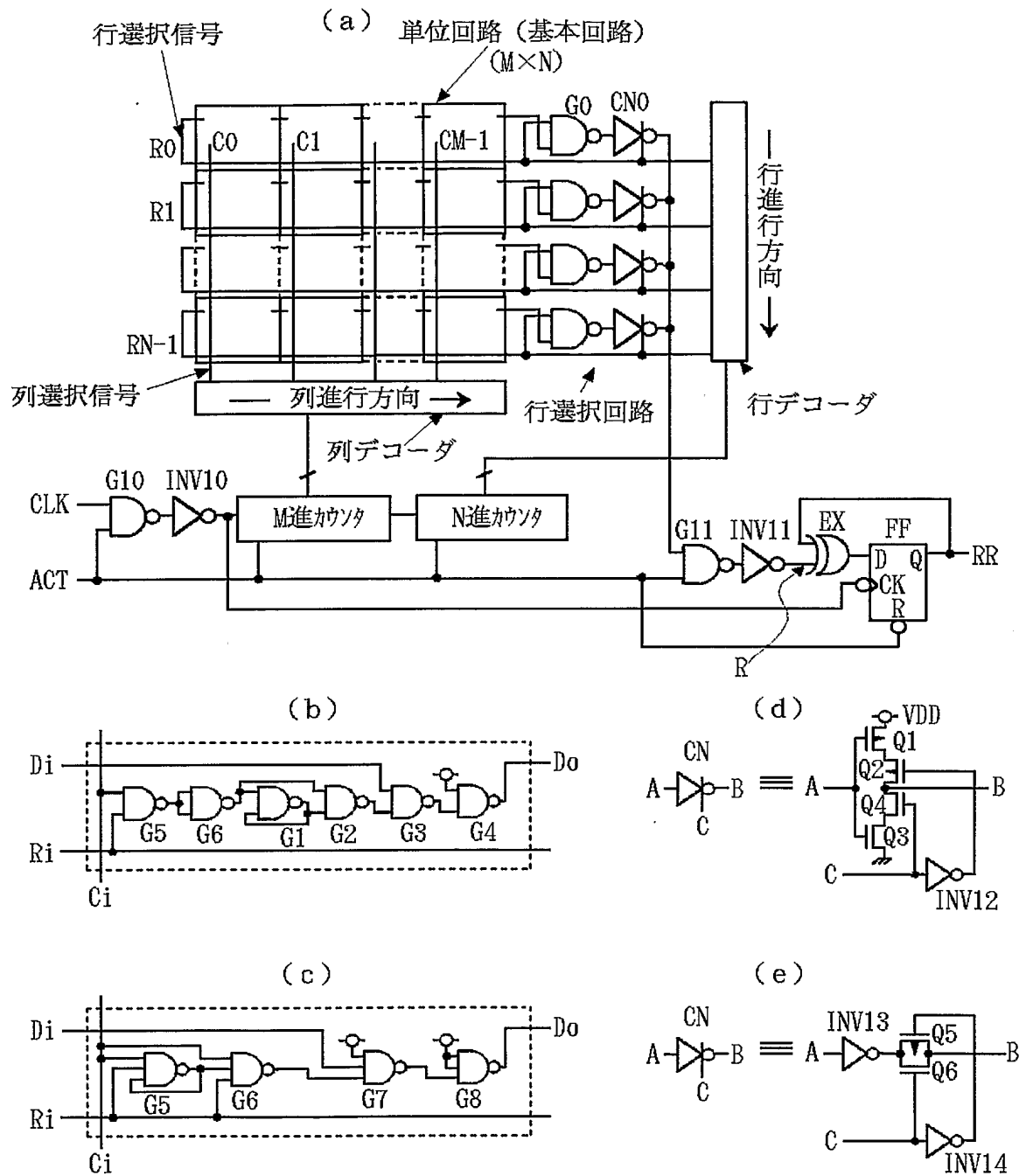
第 7 图



第 8 図

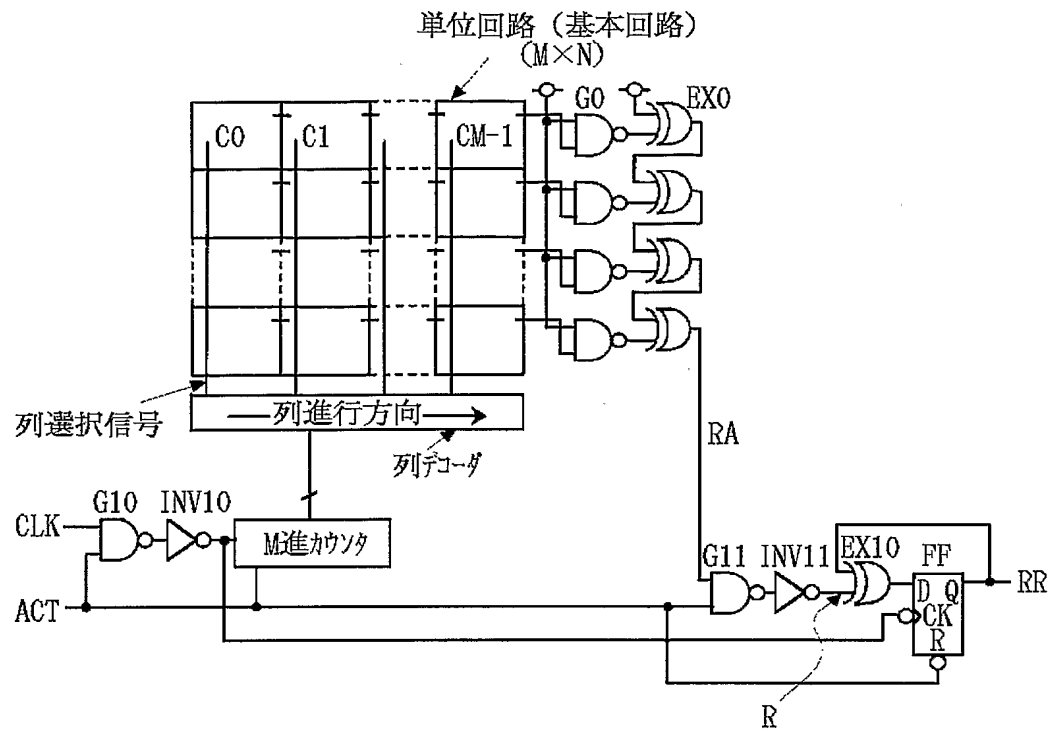


第 9 図

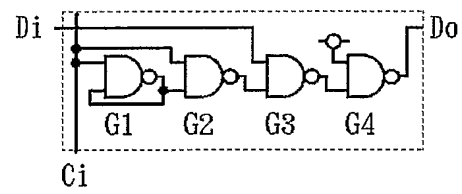


第 10 図

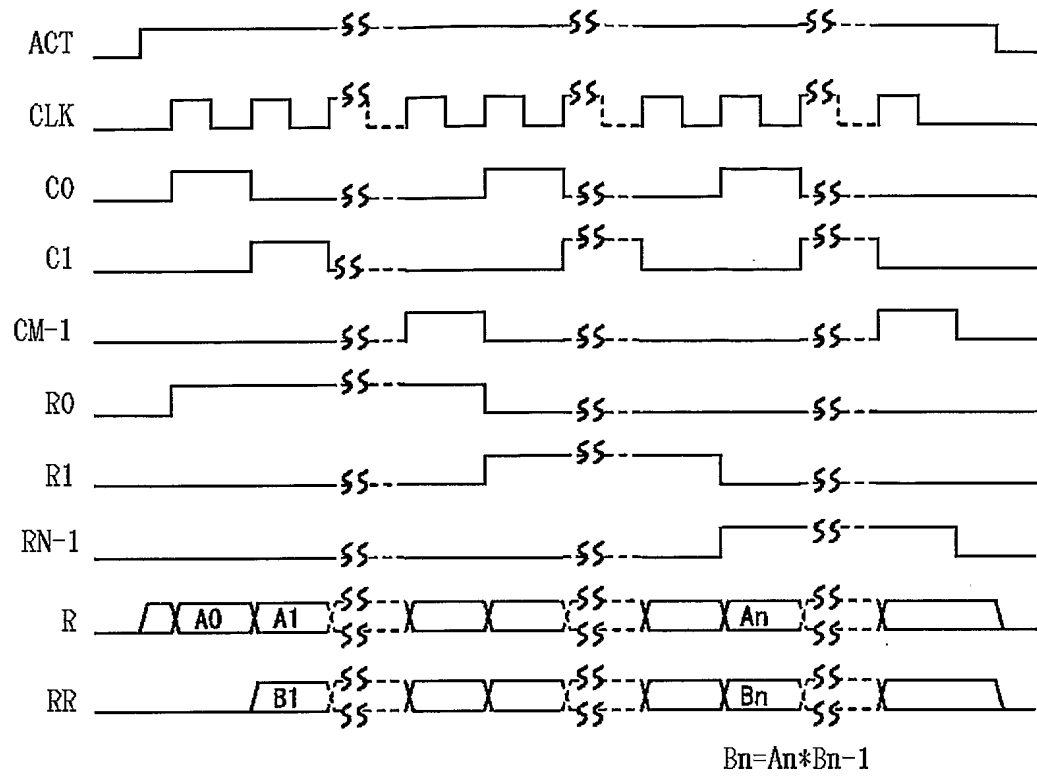
(a)



(b)

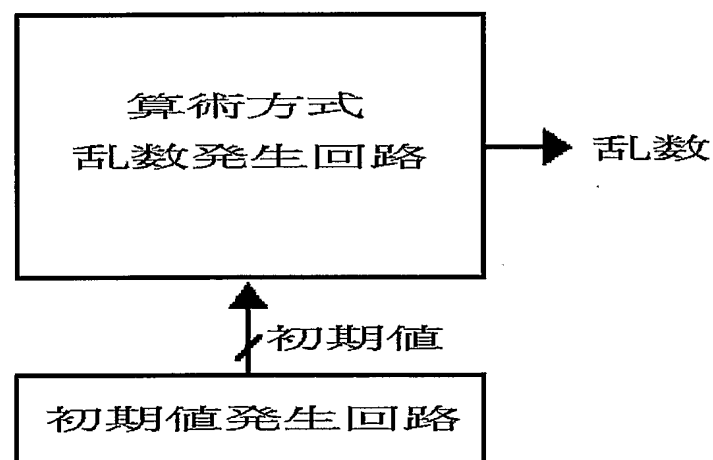


第 1 1 図

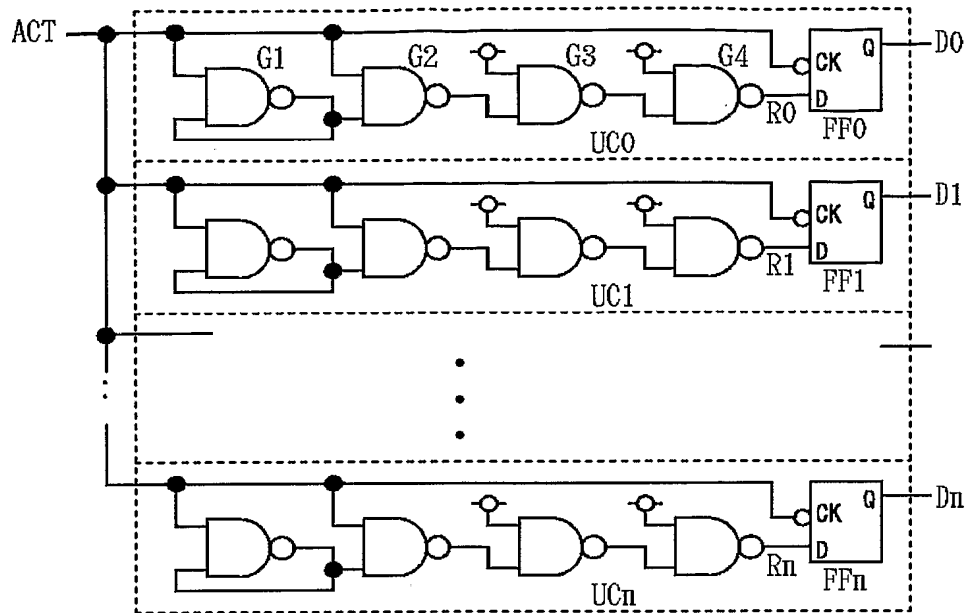


$$Bn = An * Bn - 1$$

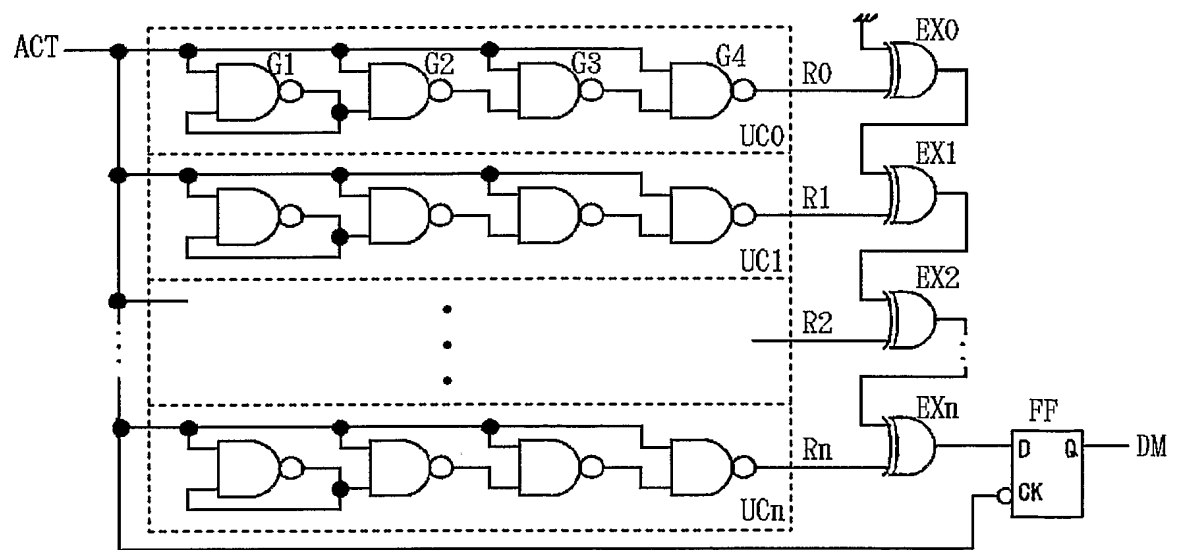
第 1 2 図



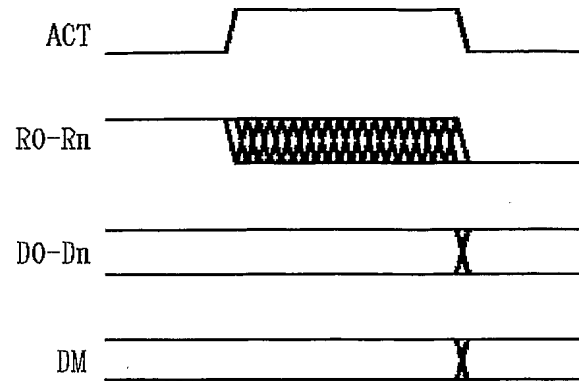
第 1 3 图



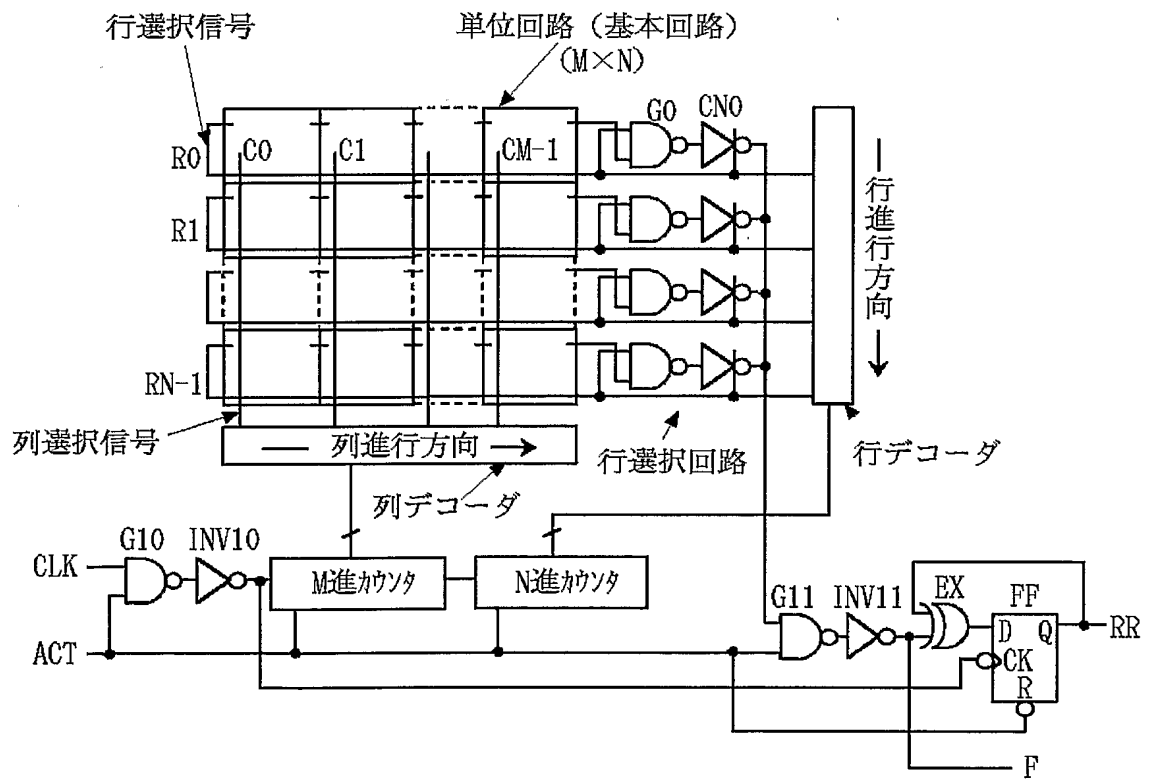
第 1 4 图



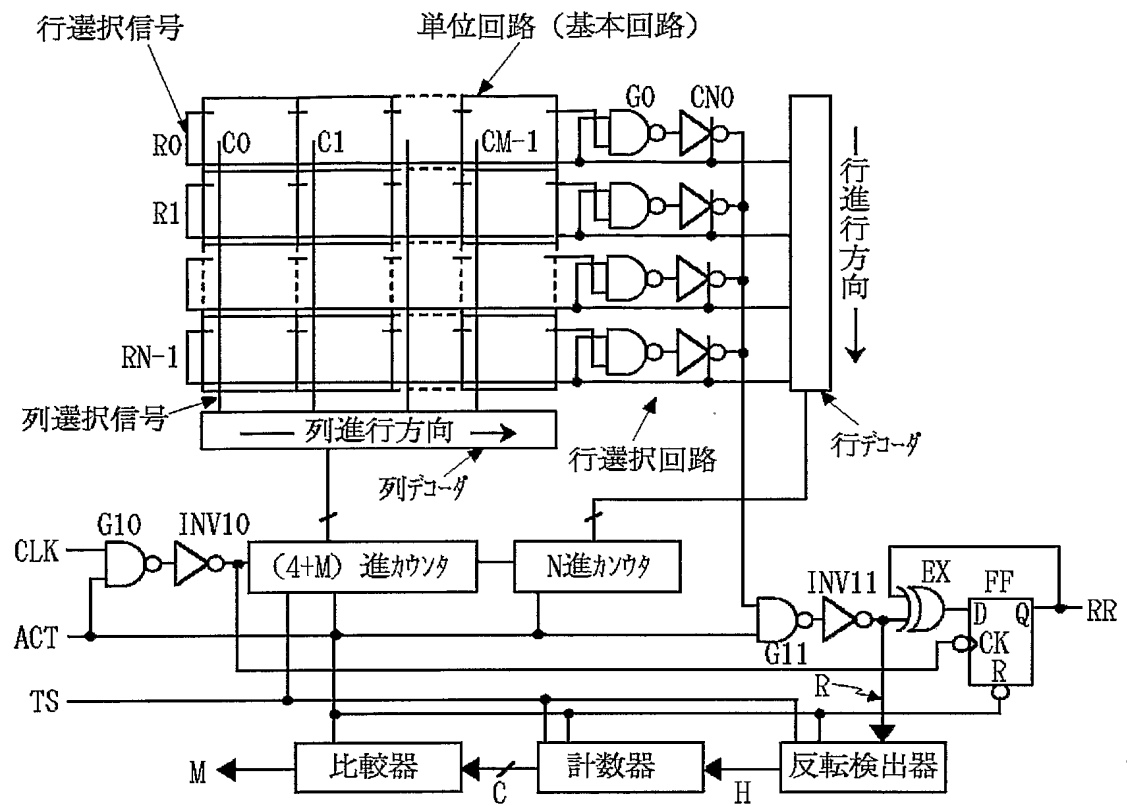
第 1 5 図



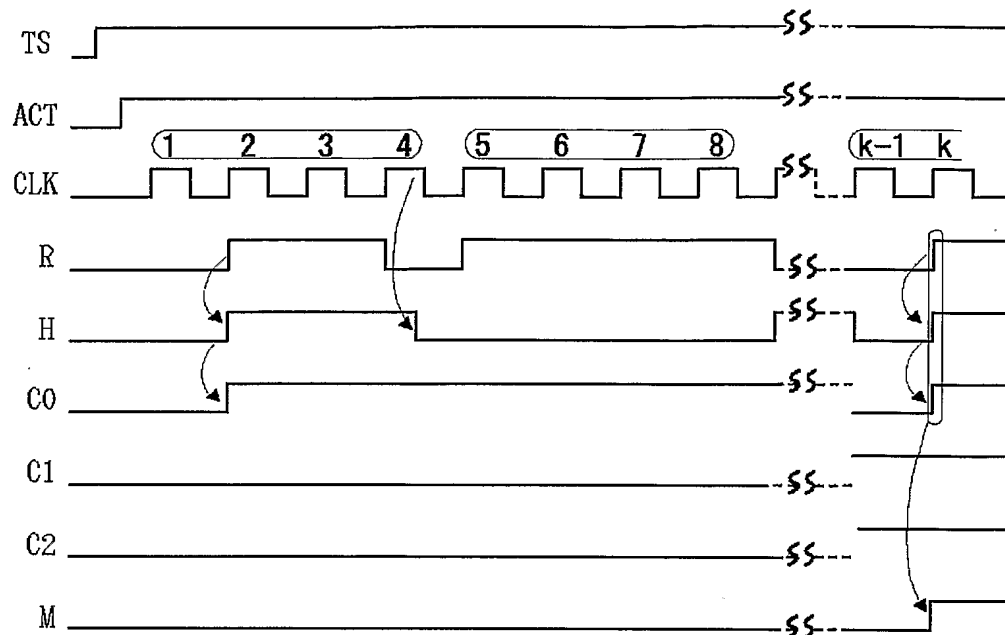
第 1 6 図



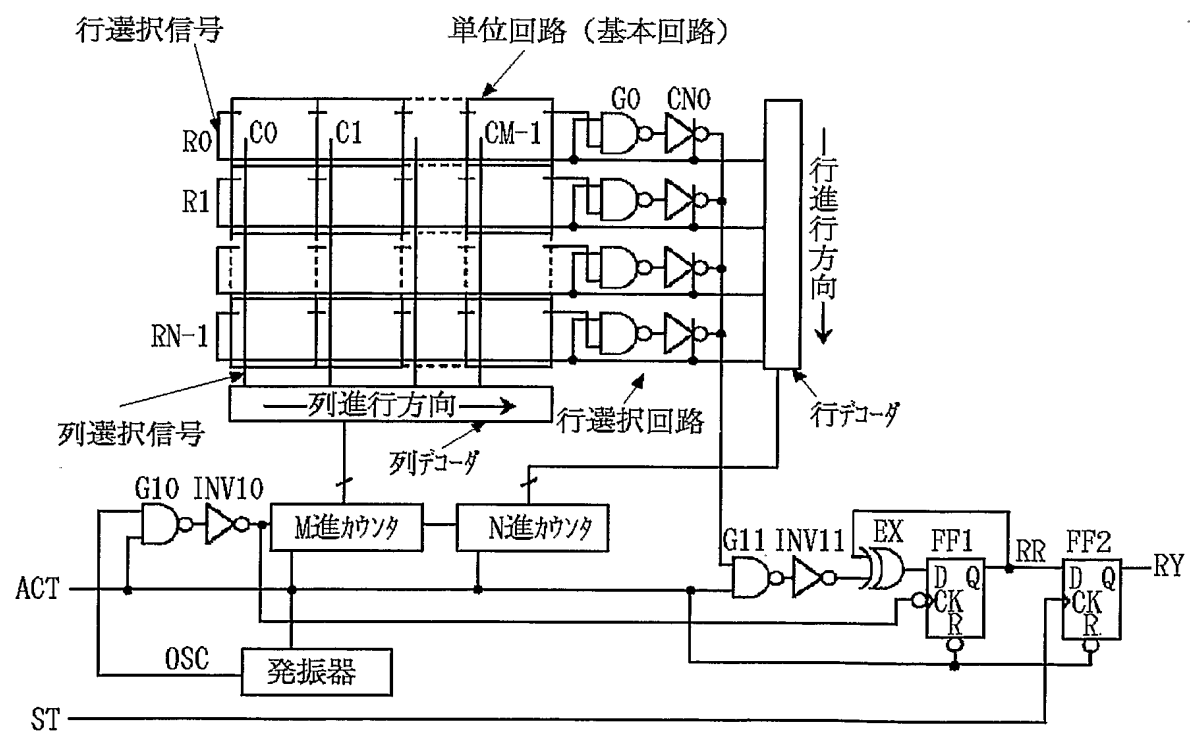
第 1 7 図



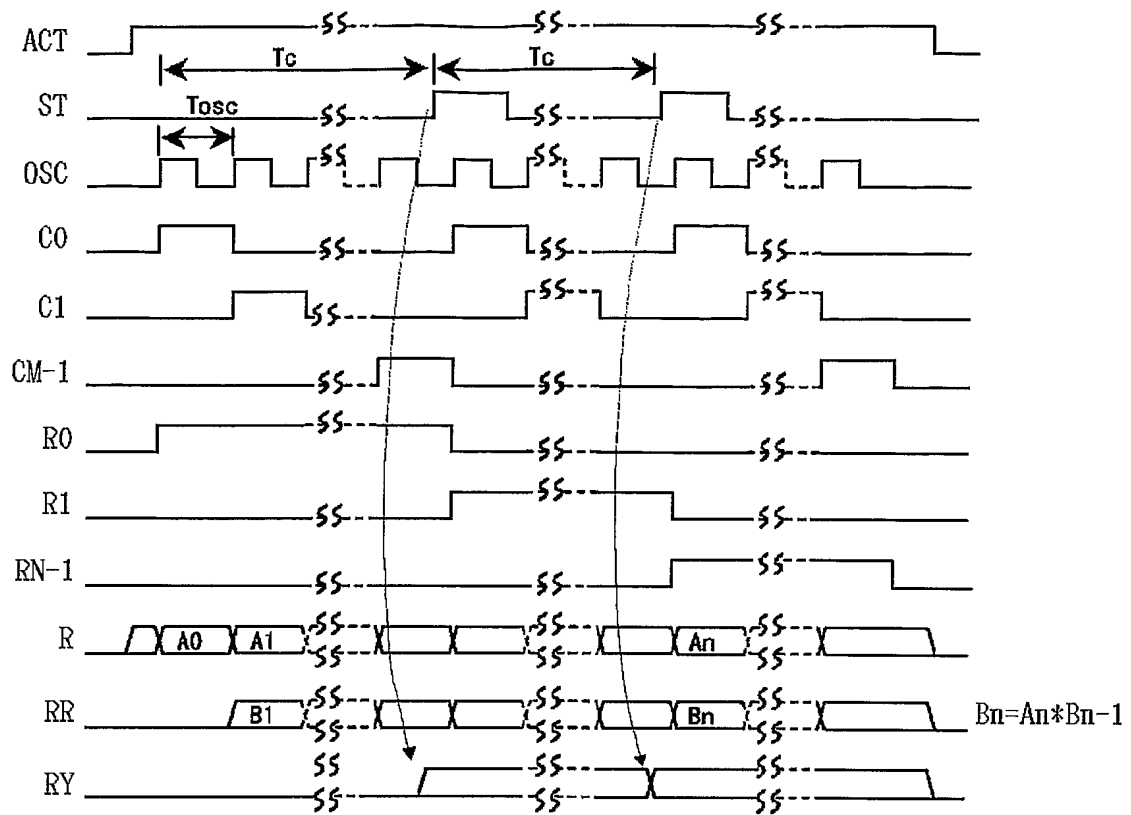
第 18 図



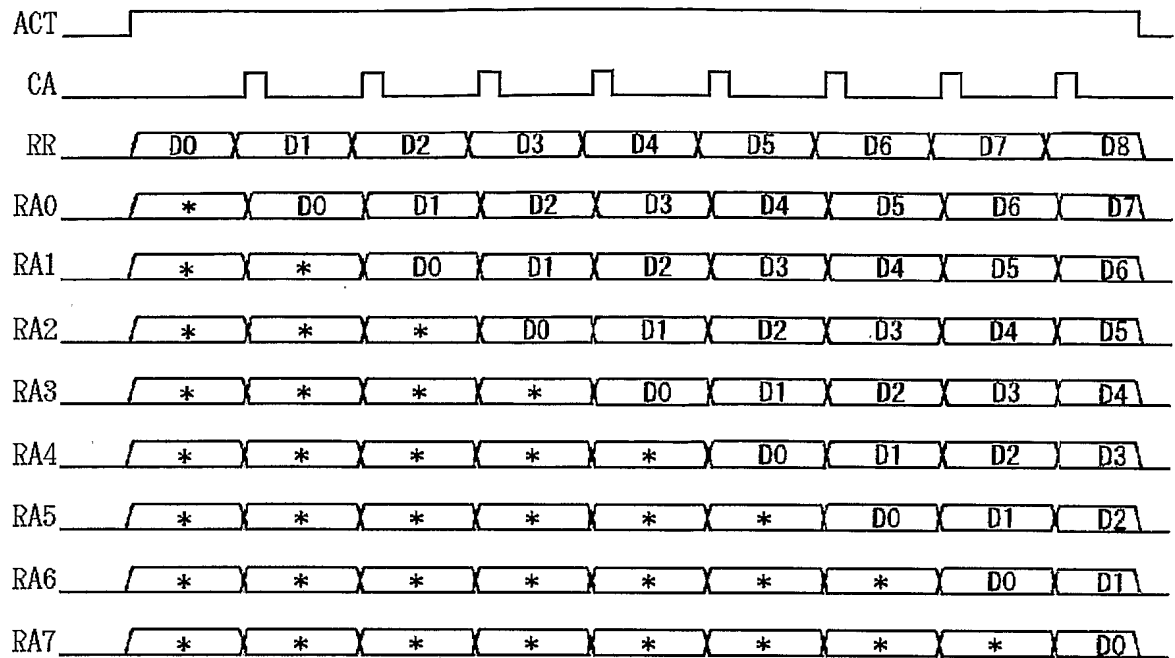
第 19 図



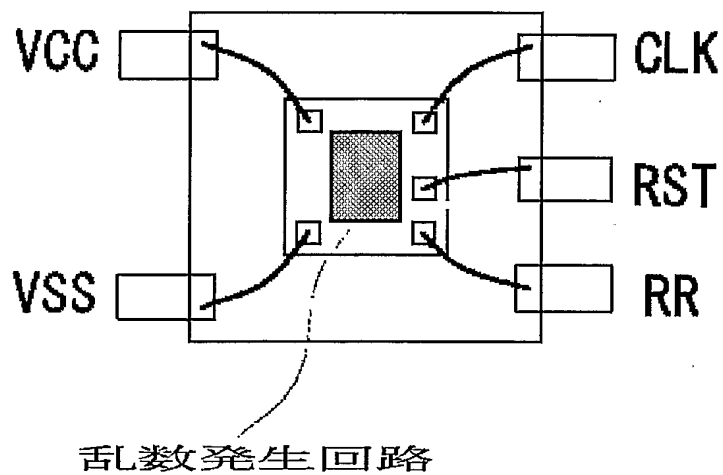
第 20 図



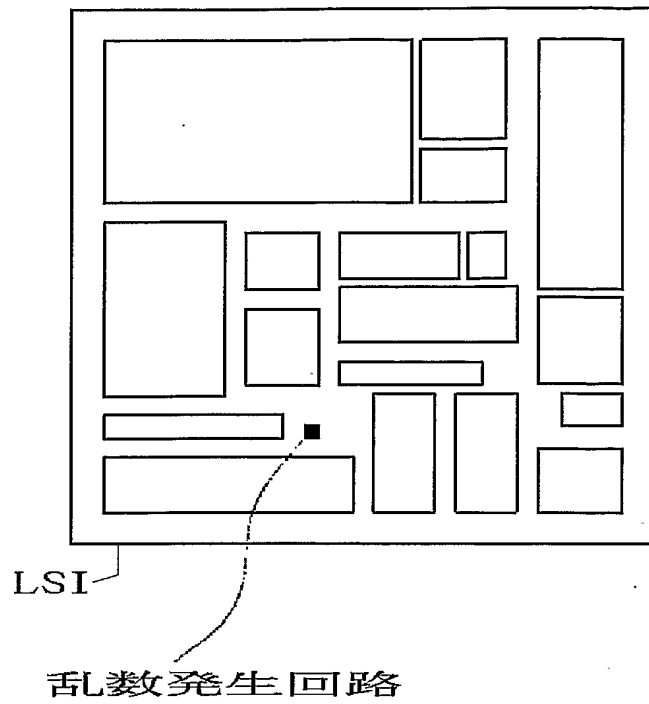
第 2 3 図



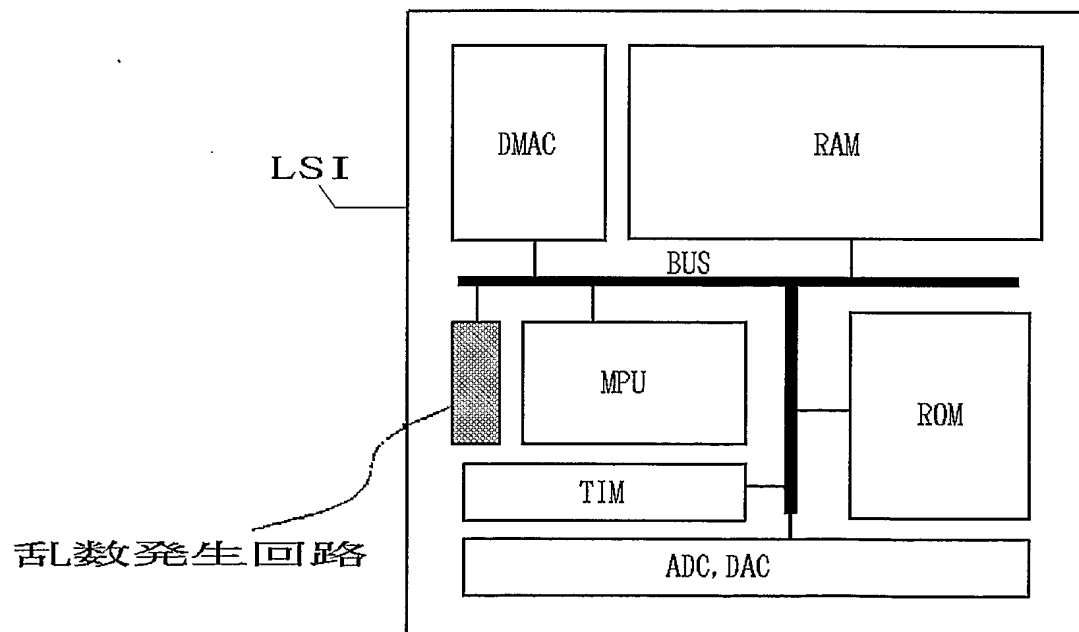
第 2 4 図



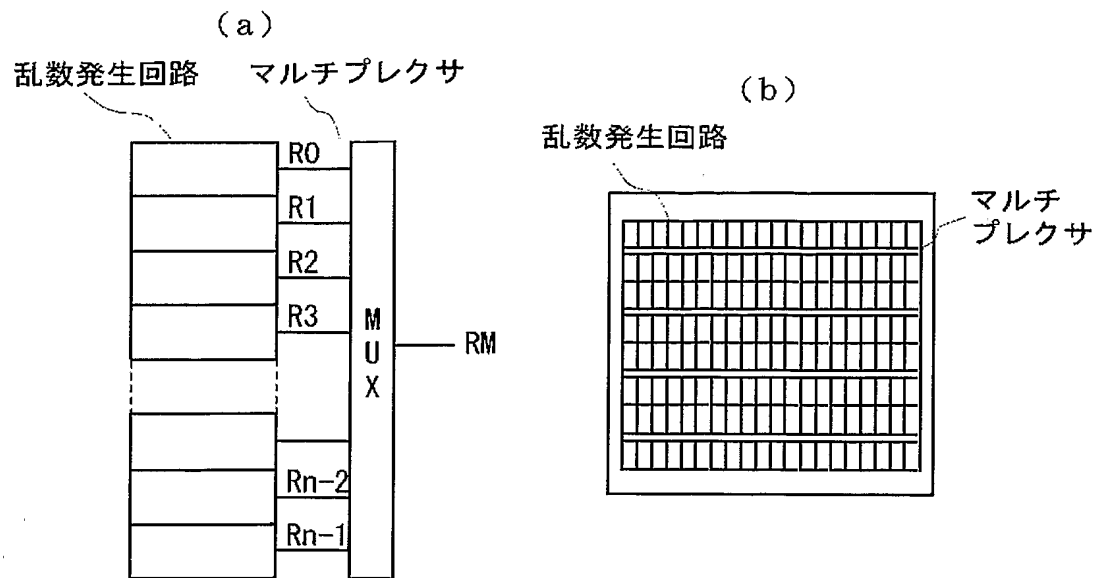
第 2 5 図



第 2 6 図



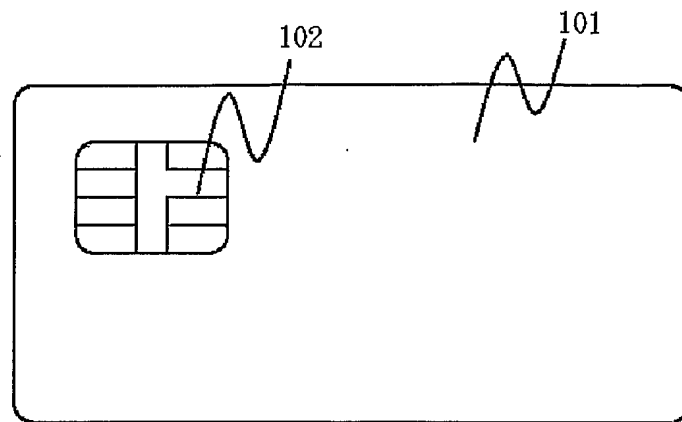
第 2 7 図



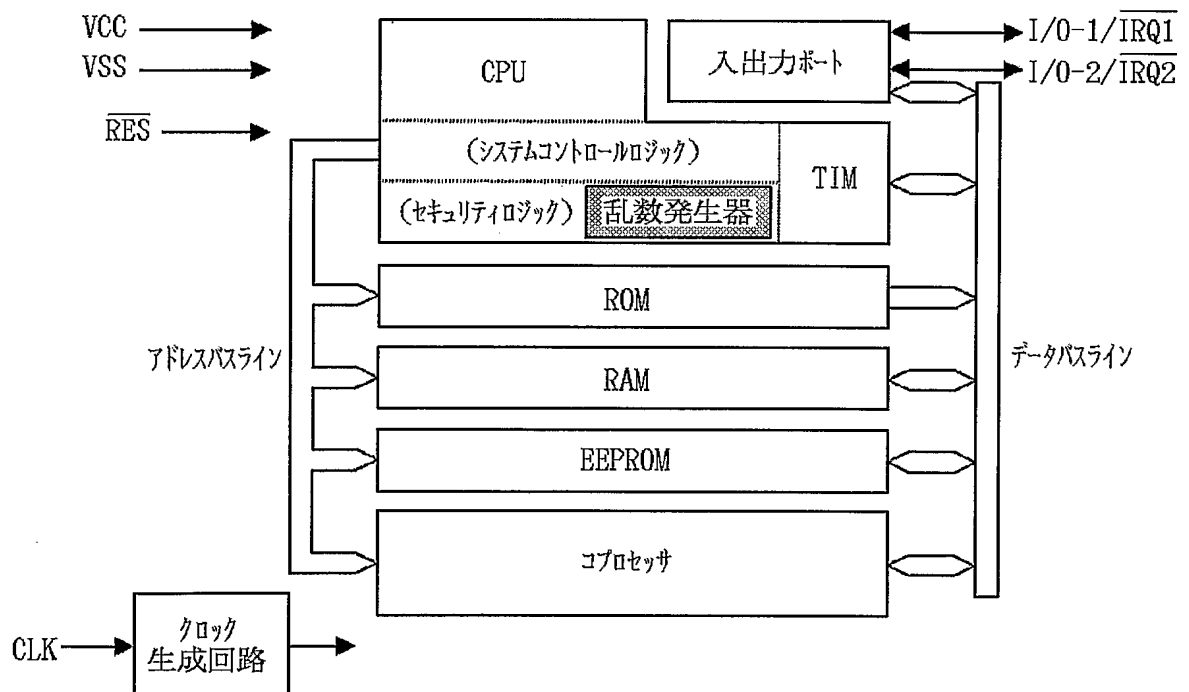
第 2 8 図



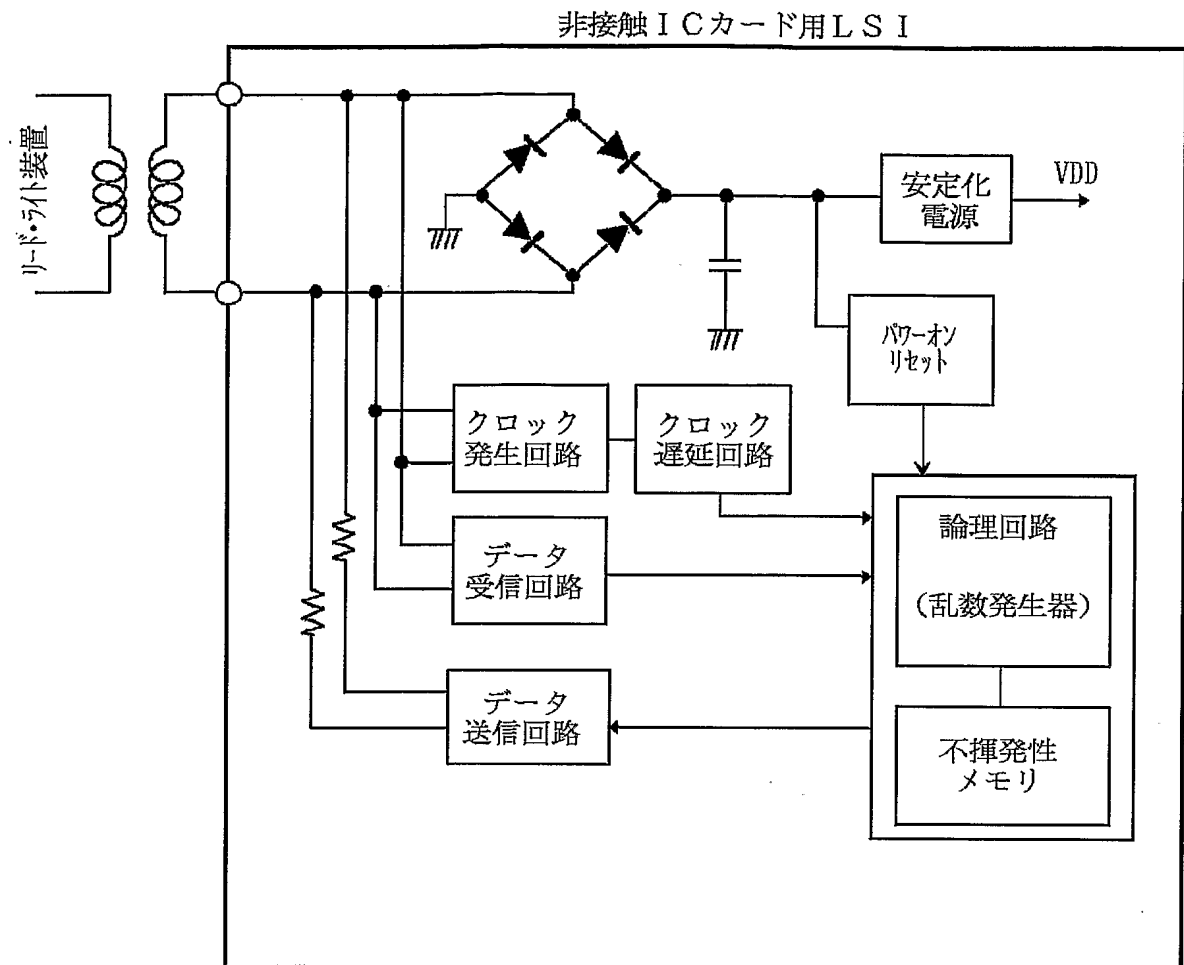
第 29 図



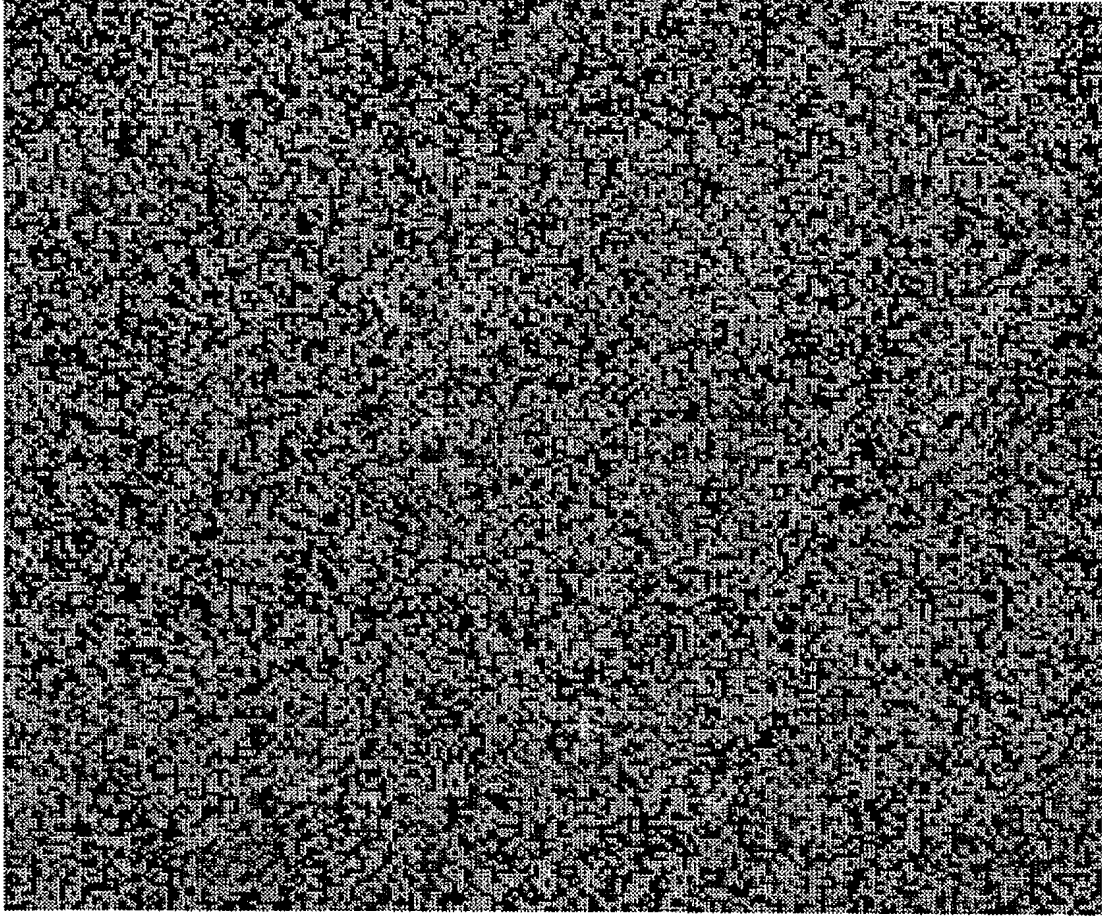
第 30 図



第 3 1 図

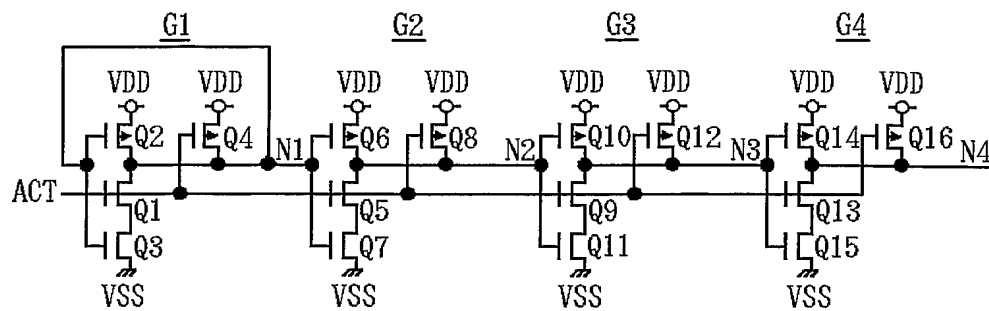


第 3 2 図

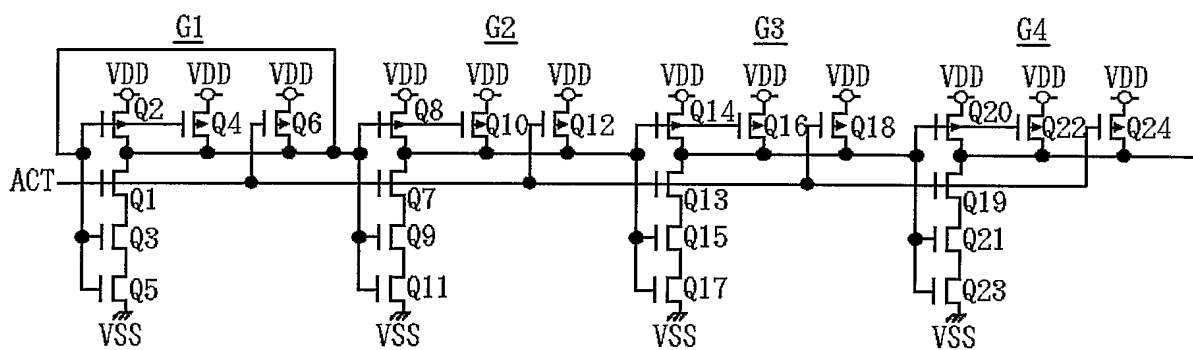


第 3 3 图

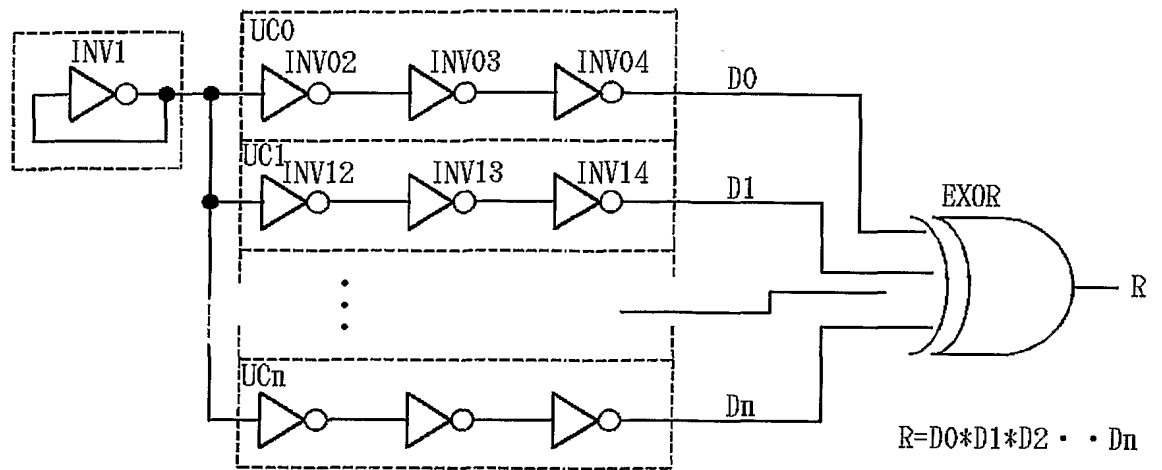
(a)



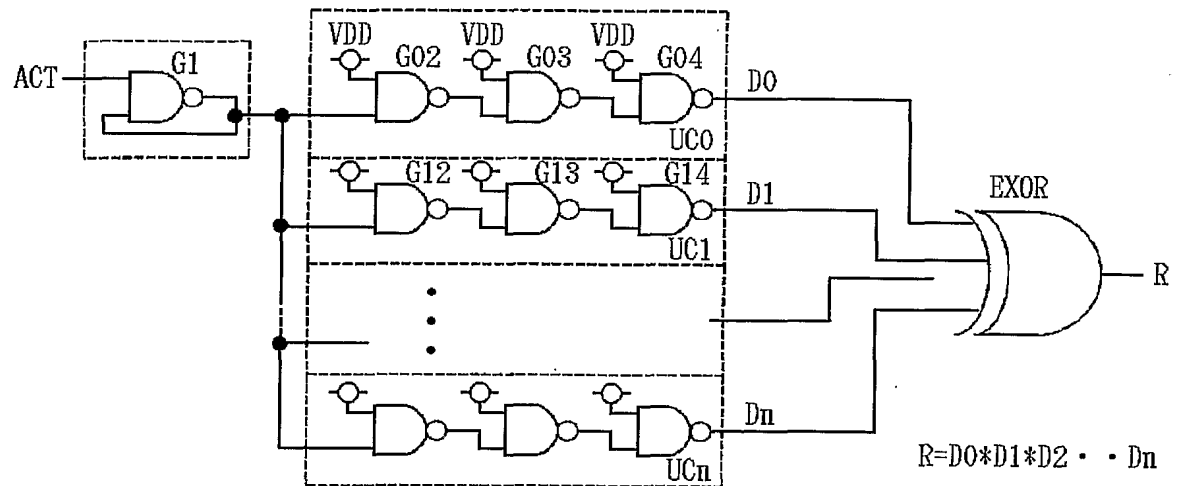
(b)



第 3 4 图



第 3 5 图



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/001486

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F7/58, H03K3/84

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-332452 A (Kabushiki Kaisha Runesasu Technology), 21 November, 2003 (21.11.03), Full text; all drawings (Family: none)	1-6, 7, 8-12
Y	WO 2002/045139 A (Kabushiki Kaisha Runesasu Technology), 06 June, 2002 (06.06.02), Full text; all drawings & EP 1341214 A1 & US 2004/0053429 A1	1-6, 7, 8-12
Y	US 5963104 A (VLSI Technology, Inc.), 05 October, 1999 (05.10.99), Full text; all drawings (Family: none)	1-6, 7, 8-12

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

11 May, 2004 (11.05.04)

Date of mailing of the international search report

25 May, 2004 (25.05.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/001486

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-108363 A (Toshiba Corp.), 11 April, 2003 (11.04.03); Full text; all drawings (Family: none)	1-2, 8-9
A	JP 2003-173254 A (Toshiba Corp.), 20 June, 2003 (20.06.03), Full text; all drawings & US 2003/0061250 A1	1-2, 8-9
A	JP 1-114211 A (SGS-Thomson Microelectronics Inc.), 02 May, 1989 (02.05.89), Full text; all drawings & EP 308294 A2	1-2, 8-9
A	WO 01/67231 A (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 13 September, 2001 (13.09.01), Full text; all drawings & US 6631390 A & JP 2003-526151 A	1-2, 8-9

A. 発明の属する分野の分類 (国際特許分類 (IPC)) <p style="text-align: center;">Int. Cl⁷ G06F 7/58</p>			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) <p style="text-align: center;">Int. Cl⁷ G06F 7/58 H03K 3/84</p>			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2004年 日本国登録実用新案公報 1994-2004年 日本国実用新案登録公報 1996-2004年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
Y	JP 2003-332452 A (株式会社ルネサステクノロジ) 2003. 11. 21, 全文、全図 (ファミリーなし)	1-6, 7, 8-12	
Y	WO 2002/045139 A (株式会社ルネサステクノロジ) 2002. 06. 06, 全文、全図 & EP 1341214 A1 & US 2004/0053429 A1	1-6, 7, 8-12	
Y	US 5963104 A (VLSI Technology, Inc.) 1999. 10. 05, 全文、全図 (ファミリーなし)	1-6, 7, 8-12	
A	JP 2003-108363 A (株式会社東芝) 2003. 0 4. 11, 全文、全図 (ファミリーなし)	1-2, 8-9	
A	JP 2003-173254 A (株式会社東芝) 2003. 0	1-2, 8-9	
<input checked="" type="checkbox"/> C欄の続きにも文献が列举されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願 の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献			
国際調査を完了した日 <p style="text-align: center;">11. 05. 2004</p>		国際調査報告の発送日 <p style="text-align: center; font-size: 1.2em;">25. 5. 2004</p>	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 山崎 慎一 電話番号 03-3581-1101 内線 3520	

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	6. 20, 全文、全図& US 2003/0061250 A1 JP 1-114211 A (エスジーエス トムソン マイクロエ レクトロニクス インク.) 1989. 05. 02, 全文、全図 & EP 308294 A2	1-2, 8-9
A	WO 01/67231 A (KONINKLIJKE PHILIPS ELECTRONICS N.V.) 2001. 09. 13, 全文、全図& US 66313 90 A & JP 2003-526151 A	1-2, 8-9